Langage et raisonnements mathématiques

Andrei Teleman
Département de mathématiques, Aix-Marseille Université

2 janvier 2022

Je remercie Clément Verrier pour son aide à la rédaction et l'amélioration du texte de ce cours.

Table des matières

1 Éléments de logique

1.1 Disjonction et conjonction

La *disjonction* $P \vee Q$ de deux propositions P, Q est vraie quand l'une des deux propositions est vraie et est fausse quand les deux propositions sont fausses. Donc la disjonction logique correspond au mot français OU au sens non-exclusif (inclusif). La table de vérité de la "disjonction" de deux propositions P, Q est

P	Q	$P \vee Q$
vraie	vraie	vraie
vraie	fausse	vraie
fausse	vraie	vraie
fausse	fausse	fausse

.

La *conjonction* $P \wedge Q$ de deux propositions P, Q est vraie quand les deux proposition sont simultanément vraies et est fausse quand (au moins) une des deux propositions est fausse. Donc la conjonction logique correspond au mot français ET. La table de vérité de la "conjonction" de deux propositions P, Q est

P	Q	$P \wedge Q$
vraie	vraie	vraie
vraie	fausse	fausse
fausse	vraie	fausse
fausse	fausse	fausse

.

La négation $\neg P$ d'une proposition P est vraie si P est fausse et est fausse si P est vraie. Donc la négation est définie par la table de vérité

P	$\neg P$
vraie	fausse
fausse	vraie

.

Remarque 1.1 Les opérations logiques $\vee$, $\wedge$, $\neg$ sont reliées par les équivalences logiques suivantes :

— *Règles d'idempotence* :
- $\neg\neg P$ équivalent à P (idempotence de la négation).
- $P \vee P$ équivalent à P (idempotence du "ou").
- $P \wedge P$ équivalent à P (idempotence du "et").

— *Règles de commutativité* :
- $P \vee Q$ équivalent à $Q \vee P$ (commutativité du "ou").
- $P \wedge Q$ équivalent à $Q \wedge P$ (commutativité du "et").

— *Règles d'associativité* :
- $(P \vee Q) \vee R$ équivalent à $P \vee (Q \vee R)$ (associativité du "ou").
- $(P \wedge Q) \wedge R$ équivalent à $P \wedge (Q \wedge R)$ (associativité du "et").

— *Lois de De Morgan en logique :*
- $\neg(P \vee Q)$ équivalent à $(\neg P) \wedge (\neg Q)$ (la négation d'une disjonction est la conjonction des négations).
- $\neg(P \wedge Q)$ équivalent à $(\neg P) \vee (\neg Q)$ (la négation d'une conjonction est la disjonction des négations).

— *Règles de distributivité* :
- $P \vee (Q \wedge R)$ équivalent à $(P \vee Q) \wedge (P \vee R)$ (distributivité de "ou" par rapport à "et").
- $P \wedge (Q \vee R)$ équivalent à $(P \wedge Q) \vee (P \wedge R)$ (distributivité de "et" par rapport à "ou").

1.2 Implication

Soient P, Q deux propositions. L'implication $P \Rightarrow Q$ est équivalente à la disjonction $\neg P \vee Q$. Donc l'implication $P \Rightarrow Q$ est vraie si et seulement si l'hypothèse P est fausse ou la conclusion Q est vraie ; cette

implication est fausse si et seulement si l'hypothèse P est vraie et la conclusion Q est fausse. La table de vérité de l'implication $P \Rightarrow Q$ est donc :

P	Q	$P \Rightarrow Q$
vraie	vraie	vraie
vraie	fausse	fausse
fausse	vraie	vraie
fausse	fausse	vraie

Exemple 1.2 Soit $\mathcal{G}$ l'ensemble des étudiants (ici présents) de ce groupe. La proposition

$$\forall x \in \mathcal{G} \ \big(x \text{ est de nationalité chinoise} \Rightarrow x \text{ est né en 1960}\big)$$

est vraie (bien qu'aucun étudiant de ce groupe n'est né en 1960). En effet, pour tout $x \in \mathcal{G}$ l'hypothèse "x est de nationalité chinoise" est fausse, donc l'implication est vraie.

L'équivalence entre $P \Rightarrow Q$ et $\neg P \vee Q$ nous donne la règle de négation d'une implication. La négation $\neg(P \Rightarrow Q)$ de l'implication $P \Rightarrow Q$ est équivalente à $\neg(\neg P \vee Q)$, qui (en tenant compte des équivalences ci-dessus) est équivalente à $P \wedge \neg Q$. *Conclusion* : la négation de l'implication $P \Rightarrow Q$ est équivalente à la conjonction $P \wedge \neg Q$.

Négation et quantificateurs. Soit $\mathcal{G}$ l'ensemble des étudiants (ici présents) de ce groupe. La négation de la proposition

$$\forall x \in \mathcal{G} \ \big(x \text{ est de nationalité française}\big)$$

est

$$\exists x \in \mathcal{G} \ \big(x \text{ n'est pas de nationalité française}\big).$$

En général, nous avons les règles de négation suivantes :

- $\neg(\forall x P(x))$ est équivalente à $\exists x(\neg P(x))$.
- $\neg(\exists x P(x))$ est équivalente à $\forall x(\neg P(x))$.

Exemple 1.3 Soit $\mathcal{G}$ l'ensemble des étudiants (ici présents) de ce groupe. La négation de la proposition

$$P : \ \forall x \in \mathcal{G} \ \big(x \text{ est de nationalité chinoise} \Rightarrow x \text{ est né en 1960}\big)$$

est

$$\neg P : \ \exists x \in \mathcal{G} \ \neg\big(x \text{ est de nationalité chinoise} \Rightarrow x \text{ est né en 1960}\big)$$

En tenant compte de la règle de négation d'une implication, on obtient

$$\neg P : \ \exists x \in \mathcal{G} \ \big(x \text{ est de nationalité chinoise} \wedge x \text{ n'est pas né en 1960}\big).$$

Cette proposition est fausse, parce qu'aucun étudiant de ce groupe n'est de nationalité chinoise.

1.3 Contraposée et réciproque

La contraposée d'une implication $P \Rightarrow Q$ est l'implication $\neg Q \Rightarrow \neg P$.

Remarque 1.4 La contraposée d'une implication est équivalente à l'implication donnée.

En effet, l'implication $\neg Q \Rightarrow \neg P$ est équivalente à $\neg\neg Q \vee \neg P$, donc à $Q \vee \neg P$, donc à $\neg P \vee Q$, donc à $P \Rightarrow Q$. Quelles équivalences connues ont été utilisées dans cette démonstration ?

Sur cette remarque s'appuie une méthode de démonstration très importante : le raisonnement par contraposée. Au lieu de démontrer directement l'implication $P \Rightarrow Q$, on démontre l'implication $\neg Q \Rightarrow \neg P$, donc on suppose que la conclusion Q est fausse et on arrive à une assertion qui contredit l'hypothèse P. Donner un exemple de démonstration par contraposée.

Plus généralement, une démonstration par l'absurde (par "reductio ad absurdum") d'un théorème énoncé sous la forme $H \Rightarrow C$ (l'hypothèse H implique la conclusion C) utilise la méthode suivante : on démontre que la conjonction $H \wedge \neg C$ amène à une contradiction (donc que cette conjonction este fausse). Donner un exemple de démonstration par l'absurde.

Exemple 1.5 Soient d_1, d_2, δ droites dans le plan euclidien. Si $d_1 \parallel \delta$ et $d_2 \parallel \delta$, alors $d_1 \parallel d_2$.

Démonstration: Par l'absurde : si les droites d_1, d_2 ne sont pas parallèles (c'est à dire si elles sont sécantes), on aura deux droites parallèles à δ qui sont distinctes et passent par un point du plan. Ceci contredit l'axiome des parallèles. ■

La *réciproque* d'une implication $P \Rightarrow Q$ est l'implication $Q \Rightarrow P$. Donc l'hypothèse de la réciproque d'une implication est la conclusion de l'implication donnée et vice-versa. En général une implication et sa réciproque ne sont pas équivalentes. Il n'y a aucune règle générale qui permet de comparer une implication avec sa réciproque. Par exemple la proposition

$$(\Gamma \text{ est rectangle}) \Rightarrow (\Gamma \text{ est parallélogramme})$$

(concernant un quadrilatère Γ) est vraie, mais la réciproque est fausse.

2 Ensembles. Opérations avec les ensembles

2.1 Ensembles. Egalité d'ensembles et inclusion

Un ensemble est une collection d'éléments. Si x est élément de l'ensemble A, alors on écrit $x \in A$ et on lit "x appartient à A". Dans le cas contraire on écrit $x \notin A$. Deux ensembles A, B sont égaux si et seulement si ils ont les mêmes éléments, donc si et seulement si

$$\forall x \ (x \in A \Leftrightarrow x \in B).$$

Un ensemble A est dit sous-ensemble (ou partie) de E si tout élément de A est élément de E, donc si

$$\forall x \ (x \in A \Rightarrow x \in E).$$

Si c'est le cas on va écrire $A \subset E$ et on va lire "A est inclus dans E".

Souvent on omet le quantificateur $\forall x$ devant une implication ou une double implication qui dépend de x. Donc $A = B$ sont égaux si et seulement si l'équivalence

$$x \in A \Leftrightarrow x \in B$$

est vraie et $A \subset E$ si et seulement si l'implication

$$x \in A \Rightarrow x \in E$$

est vraie. Dans ces propositions le quantificateur $\forall x$ devant l'implication est sous-entendu.

Remarque 2.1 Soient A, B deux ensembles. $A = B$ si et seulement si $A \subset B$ et $B \subset A$.

Sur cette remarque s'appuie la méthode "par double inclusion" : pour démontrer que deux ensembles A, B sont égaux, on démontre d'abord que tout élément de A est élément de B (que $A \subset B$), puis que tout élément de B est élément de A (que $B \subset A$).

On peut définir un ensemble en indiquant la "liste" de ses éléments. S'il s'agit d'un ensemble fini, on peut écrire cette liste explicitement entre accolades, par exemple :

$$A = \{3, 5, 11, 25\}.$$

L'ordre des éléments dans la liste ne joue aucun rôle, donc on a

$$A = \{3, 5, 11, 25\} = \{5, 3, 11, 25\} = \{11, 25, 3, 5\} = \dots$$

Dans la liste qui définit un ensemble, les répétitions (les multiplicités) ne jouent aucun rôle non plus, donc la liste $\{3, 3, 5, 5, 5, 11, 25\}$ définit le même ensemble A. En général, pour un ensemble fini donné par une liste explicite, on évite les répétitions dans la liste.

L'ensemble vide $\emptyset$ est défini par la liste vide { }, donc $\emptyset$ est l'ensemble qui n'a aucun élément. Autrement dit, l'ensemble vide est l'unique ensemble $\emptyset$ pour lequel la proposition

$$\forall x \ (x \notin \emptyset)$$

est vraie. En tenant compte de la définition de l'inclusion on obtient $\emptyset \subset A$ pour tout ensemble A.

Un *singleton* est un ensemble qui a un seul élément. Le singleton d'élément a s'écrit $\{a\}$. Attention à ne pas faire de confusion entre a et le singleton associé $\{a\}$.

Le *cardinal* d'un ensemble fini est le nombre d'éléments de l'ensemble. Donc, pour un ensemble A et un nombre naturel $n \in \mathbb{N}$, la formule $\text{card}(A) = n$ signifie "A est un ensemble fini à n éléments". Par exemple

$$\text{card}(\{3,\ 5,\ 11,\ 25\}) = 4.$$

Souvent on utilise les notations $|A|$ ou $\#A$ pour le cardinal de A. Notons que $\text{card}(\emptyset) = 0$ et le cardinal d'un singleton $\{a\}$ est 1.

La notion de cardinal peut être généralisée pour les ensembles infinis, mais ce formalisme dépasse les objectifs de ce cours introductif.

On peut définir un ensemble en utilisant une "liste" d'éléments définie implicitement par une propriété. La forme générale d'une telle définition est

$$A = \{x|\ P(x)\},$$

et on va lire : A est l'ensemble des éléments x ayant la propriété $P(x)$ (pour lesquels $P(x)$ est vraie). Si on veut introduire le sous-ensemble de E formé des éléments x de E ayant la propriété $P(x)$, on va écrire

$$A := \{x \in E|\ P(x)\}.$$

Par exemple la formule

$$A := \{x \in \mathbb{Z}|\ \exists k \in \mathbb{Z},\ x = 2k\}$$

définit l'ensemble des nombres entiers pairs et la formule

$$A := \{x \in \mathbb{R}|\ 2 \leq x < 5\}$$

définit l'intervalle $[2, 5[$.

2.2 Lecture facultative : le paradoxe de Russel

Une question se pose : est-ce qu'on peut associer à *toute* proposition $P(X)$ dépendant d'une variable X (à tout "prédicat" $P(X)$) un ensemble défini par la formule $A := \{X|\ P(X)\}$? La réponse est négative. On va voir que, si on accepte ce principe, sans aucune restriction sur les prédicats admis, on va arriver à un paradoxe (antinomie). Considérons la proposition $X \notin X$ et supposons que l'ensemble associé $C := \{X|\ X \notin X\}$ existe. Donc C est l'ensemble des ensembles n'appartenant pas à eux-mêmes. Considérons la proposition $R :\ C \in C$.

Question : est-ce que R est vraie ?

Si R est vraie, alors C est élément de C, donc satisfait la propriété qui caractérise les éléments de C, à savoir $C \notin C$. Contradiction. Si R n'est pas vraie, alors C n'est pas élément de C, donc ne satisfait pas la propriété qui caractérise les éléments de C. Donc ce n'est pas vrai que $C \notin C$, donc $C \in C$. Contradiction.

Nous avons obtenu l'équivalence $R \Leftrightarrow \neg R$. Une théorie qui contient une telle équivalence (un paradoxe) est dite incohérente. Donc la théorie naïve des ensembles est incohérente. Le paradoxe est éliminé dans les théories axiomatiques des ensembles. La propriété $X \notin X$ est vérifiée par tous les ensembles, mais ne définit pas un ensemble. Dans la théorie axiomatique de von Neumann-Bernays-Gödel

`https://fr.wikipedia.org/wiki/Théorie_des_ensembles_de_von_Neumann-Bernays-Gödel`

la propriété $X \notin X$ définit une classe, à savoir la classe qui contient tous les ensembles en tant qu'éléments. Cette classe s'appelle la classe totale. La notion de classe est plus générale que celle d'ensemble. Une classe

est un ensemble si elle est élément d'une classe. Un prédicat $P(X)$ construit dans le cadre de la théorie définit une classe, à savoir

$$\{X \text{ ensemble}|\ P(X)\}.$$

Par exemple, pour un ensemble fixé A, la formule

$$\{X \text{ ensemble}|\ X \subset A\}$$

définit a priori une classe. Un axiome important de théorie affirme que, pour tout ensemble A, cette classe est un ensemble ; cet ensemble s'appelle l'ensemble des parties de A (voir la section 2.4).

2.3 Réunion, intersection, différence ensembliste

Pour deux ensembles A, B on définit *la réunion* $A \cup B$, *l'intersection* $A \cap B$, et *la différence ensembliste* $A \setminus B$ par les formules

$$A \cup B := \{x|\ (x \in A) \vee (x \in B)\},\ A \cap B := \{x|\ (x \in A) \wedge (x \in B)\},\ A \setminus B := \{x|\ (x \in A) \wedge (x \notin B)\}.$$

La différence ensembliste $A \setminus B$ s'appelle "A privé de B", donc on évite le mot "moins" utilisé pour la différence des nombres.

Si A est un sous-ensemble de E, on définit le complémentaire de A (par rapport à E) par la formule

$${}^cA := \{x \in E|\ x \notin A\} = E \setminus A.$$

Dans la notation ${}^cA$ l'ensemble E n'est pas indiqué. On a supposé donc que E a été fixé et est connu.

En utilisant les équivalences logiques mentionnées dans la remarque 1.1 on obtient facilement les identités suivantes pour les opérations avec les ensembles :

Remarque 2.2
1. Soient E un ensemble et A un sous-ensemble de E. Alors ${}^c({}^cA) = A$ (idempotence du passage au complémentaire).
2. Soit A un ensemble. Alors
   (a) $A \cup A = A$ (idempotence de la réunion).
   (b) $A \cap A = A$ (idempotence de l'intersection).
3. Soient A, B deux ensembles. Alors
   (a) $A \cup B = B \cup A$ (la commutativité de la réunion).
   (b) $A \cap B = B \cap A$ (la commutativité de l'intersection).
4. Soient A, B, C trois ensembles. Alors
   (a) $(A \cup B) \cup C = A \cup (B \cup C)$ (l'associativité de la réunion).
   (b) $(A \cap B) \cap C = A \cap (B \cap C)$ (l'associativité de l'intersection).
5. *Lois de De Morgan en théorie des ensembles :* Soient A, B deux sous-ensembles de E. Alors
   (a) ${}^c(A \cup B) = {}^cA \cap {}^cB$ (le complémentaire de la réunion est l'intersection des complémentaires).
   (b) ${}^c(A \cap B) = {}^cA \cup {}^cB$ (le complémentaire de l'intersection est la réunion des complémentaires).
6. Soient A, B, C trois ensembles. Alors
   (a) $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ (la distributivité de l'intersection par rapport à la réunion).
   (b) $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ (la distributivité de la réunion par rapport à l'intersection).

Réunion et intersection d'une famille d'ensembles Soit I un ensemble, qui sera appelé ensemble d'indices. Une famille d'ensembles indexée par I est la donnée pour tout $i \in I$ d'un ensemble A_i. Une telle famille est notée $(A_i)_{i \in I}$. On définit la réunion de la famille $(A_i)_{i \in I}$ par

$$\bigcup_{i \in I} A_i = \{x|\ \exists i \in I,\ x \in A_i\},$$

et (pour $I \neq \emptyset$) on définit l'intersection de la famille $(A_i)_{i \in I}$ par

$$\bigcap_{i \in I} A_i = \{x|\ \forall i \in I,\ x \in A_i\}.$$

Exemple 2.3 Considérons les familles d'intervalles $(]-n,n[)_{n\in\mathbb{N}^*}$, $(]-\frac{1}{n},\frac{1}{n}[)_{n\in\mathbb{N}^*}$. Nous avons

$$\bigcup_{n\in\mathbb{N}^*}]-n,n[=\mathbb{R}\,,\ \bigcap_{n\in\mathbb{N}^*}\left]-1-\frac{1}{n},1+\frac{1}{n}\right[=[-1,1].$$

$$\bigcup_{n\in\mathbb{N}^*}\left[-1+\frac{1}{n},1-\frac{1}{n}\right]=]-1,1[\,,\ \bigcap_{n\in\mathbb{N}^*}\left]-\frac{1}{n},\frac{1}{n}\right[=\{0\}.$$

Justifier ces égalités.

2.4 L'ensemble des parties d'un ensemble

Soit E un ensemble. L'ensemble des parties $\mathcal{P}(E)$ de E est défini par

$$\mathcal{P}(E) := \{A \text{ ensemble}|\ A\subset E\}.$$

(voir la section 2.2). Donc les *éléments* de $\mathcal{P}(E)$ sont les *sous-ensembles* de E. Si $A\subset E$, alors A va jouer un double rôle : *sous-ensemble* de E et *élément* de $\mathcal{P}(E)$. Par exemple

$$\mathcal{P}(\{0,1\})=\{\emptyset,\{0\},\{1\},\{0,1\}\}.$$

En utilisant la récurrence par rapport à n, on peut démontrer :

Proposition 2.4 *Soient E un ensemble fini de cardinal n, $k\in\{0,1,\dots,n\}$ et $\mathcal{P}_k(E)$ l'ensemble des parties de cardinal k de E. Alors*

1. $\mathrm{card}(\mathcal{P}(E))=2^n$.
2. $\mathrm{card}(\mathcal{P}_k(E))=\binom{n}{k}$.

2.5 Couples. Produit cartésien.

On va utiliser la notation (a,b) pour désigner *le couple* (*la paire ordonnée*) formé(e) de a et de b. La notion de couple est caractérisée par la règle suivante qui nous permet de décider si deux couples sont égaux :

$$(a,b)=(a',b')\Leftrightarrow(a=a')\wedge(b=b').$$

Donc, dans un couple, on tient compte de l'ordre des éléments. Plus précisément
- Si $a\neq b$ alors $(a,b)\neq(b,a)$ bien que $\{a,b\}=\{b,a\}$.
- Si $a=b$, alors $\{a,a\}=\{a\}$ (donc $\{a,a\}$ est un singleton), mais le couple (a,a) ne peut pas être écrit en faisant intervenir a une seule fois.

Remarque 2.5

1. On peut se poser la question de savoir si on peut introduire la notion de couple dans le cadre de la théorie des ensembles, donc sans utiliser des notions extérieures à cette théorie. La réponse est positive, mais ce formalisme, développé par Kuratowski, dépasse les objectifs de ce chapitre, donc nous ne l'utiliserons pas dans la suite. Nous mentionnons seulement que, d'après Kuratowski, le couple (a,b) est défini par la formule $(a,b):=\big\{\{a\},\{a,b\}\big\}$. On remarque qu'avec cette définition, on a bien l'équivalence
$$(a,b)=(a',b')\Leftrightarrow(a=a')\wedge(b=b')$$
et le couple (a,b) est un objet défini dans le cadre de la théorie des ensembles.
2. De la même manière on peut introduire la notion de triplet, quadruplet, ou, plus généralement, n-uplet. Par exemple (a,b,c) désigne le triplet formé des éléments a, b, c. La notion de triplet sera caractérisée par la règle
$$(a,b,c)=(a',b',c')\Leftrightarrow(a=a')\wedge(b=b')\wedge(c=c')$$
qui nous permet de décider si deux triplets sont égaux. En général pour deux n-uplets $(a_1,\dots,a_n)$, $(a'_1,\dots,a'_n)$ on a
$$(a_1,\dots,a_n)=(a'_1,\dots,a'_n)\Leftrightarrow a_i=a'_i \text{ pour } 1\leq i\leq n.$$

Définition 2.6 *Soient A, B deux ensembles. Le produit cartésien $A \times B$ est défini par*

$$A \times B := \{(a, b) |\ a \in A,\ b \in B\}.$$

Donc $A \times B$ est l'ensemble des couples dont le premier élément appartient à A et le second à B.

Remarque 2.7

1. Soient A, B, B' trois ensembles. Alors
$$A \times (B \cup B') = (A \times B) \cup (A \times B').$$
2. Soient A, A', B, B' quatre ensembles. Alors
$$(A \cap A') \times (B \cap B') = (A \times B) \cap (A' \times B').$$
3. Soient A, B deux ensembles finis. Alors
$$\mathrm{card}(A \times B) = \mathrm{card}(A) \cdot \mathrm{card}(B).$$

Exemple 2.8 Soient $A = \{2, 3, 5, 11\}$, $B = \{0, 1\}$. On a

$$A \times B = \{(2, 0), (3, 0), (5, 0), (11, 0), (2, 1), (3, 1), (5, 1), (11, 1)\}.$$

Définition 2.9 *Soit A un ensemble. La diagonale du produit cartésien $A \times A$ est définie par*

$$\Delta_A := \{(a, a) |\ a \in A\}.$$

Exercice 2.10 Soit $A := [0, 2]$. En identifiant $\mathbb{R} \times \mathbb{R}$ avec le plan euclidien (à l'aide d'un système de coordonnées), représenter par un dessin $A \times A$ et la diagonale Δ_A. Même question pour $A = \mathbb{R}$.

3 Relations

3.1 Relations entre deux ensembles

Définition 3.1 *Soient A, B deux ensembles. Une relation entre A et B est un sous-ensemble $R \subset A \times B$. Pour un couple $(a, b) \in A \times B$ on va utiliser la notation simplifiée $a\ R\ b$ au lieu de $(a, b) \in R$ et on va lire "a est en relation R avec b". Une relation entre A et A s'appelle aussi relation sur A.*

Exemple 3.2 Soit A un ensemble. La diagonale $\Delta_A \subset A \times A$ (voir la définition 2.9) est une relation sur A. Remarquer que, par rapport à cette relation, on a

$$a\ \Delta_A\ b \Leftrightarrow a = b.$$

Cette relation s'appelle la relation d'égalité sur A. Un élément $a \in A$ est en relation Δ_A avec lui-même et seulement avec lui-même.

Exemple 3.3 Soit A, B deux ensembles. Le produit cartésien $A \times B$ est une relation entre A et B. Par rapport à cette relation on constate que a est en relation avec b pour *tout* couple $(a, b) \in A \times B$.

Exemple 3.4 Soit $n \in \mathbb{N}^*$. La relation de congruence mod n est définie par

$$a \equiv b\ [n] \text{ si } b - a \text{ est divisible par } n.$$

Si $a \equiv b\ [n]$ on va dire que a, b sont congrus modulo n (ou mod n).

Rappelons le théorème de division euclidienne dans $\mathbb{Z}$:

Théorème 3.5 *(division euclidienne) Soit $n \in \mathbb{N}^*$ et $a \in \mathbb{Z}$. Il existe un unique couple $(q, r) \in \mathbb{Z} \times \mathbb{N}$ tel que*

$$a = qn + r \text{ et } 0 \leq r < n.$$

Les nombres q, r définis par ces conditions s'appellent le quotient, respectivement le reste de la division euclidienne de a par n.

Remarque 3.6 Soit $n \in \mathbb{N}^*$ et $(a, b) \in \mathbb{Z} \times \mathbb{Z}$. Alors $a \equiv b\ [n]$ si et seulement si le reste de la division euclidienne de a par n coïncide avec le reste de la division euclidienne de b par n.

Démonstration: En effet, supposons $a \equiv b\ [n]$, soit $k \in \mathbb{Z}$ tel que $b - a = kn$ et soit q, r le quotient et le reste de la division euclidienne de a par n. On obtient $b = a + kn = qn + r + kn = (k + q)n + r$ (avec $k + q \in \mathbb{Z}$ et $0 \leq r < n$), ce qui montre que le reste de la division euclidienne de b par n est le même naturel r. Réciproquement, si les deux restes coïncident, on obtient $a = qn + r$, $b = q'n + r$, donc $b - a = (q' - q)n$, donc $a \equiv b\ [n]$. ■

Exercice 3.7 Calculer le quotient et le reste de la division euclidienne de 123 par 11. La même question pour -123.

Exercice 3.8 Montrer que $123 \equiv 35\ [11]$. Utiliser d'abord la définition de la congruence mod n, puis la remarque 3.6.

Exercice 3.9 Préciser l'ensemble

$$\{x \in \mathbb{Z} |\ x \equiv 35\ [11],\ -50 \leq x \leq 150\}.$$

Exemple 3.10 Soit $A = \{1, 2, 3, 4\}$. Le sous-ensemble $R := \{(a, b) \in A \times A |\ a \leq b\}$ est une relation sur A. Dans ce cas on peut écrire R explicitement :

$$R = \{(1,1), (1,2), (1,3), (1,4), (2,2), (2,3), (2,4), (3,3), (3,4), (4,4)\}.$$

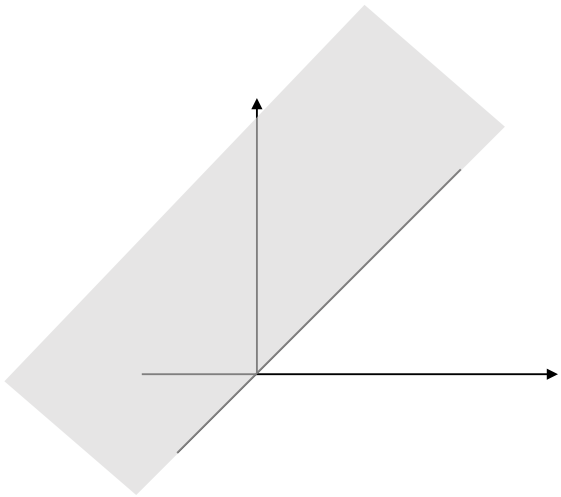


FIGURE 1 – La relation d'ordre standard $\leq$ sur $\mathbb{R}$.

Exemple 3.11 La relation d'ordre standard sur $\mathbb{R}$ est le sous-ensemble de $\mathbb{R} \times \mathbb{R}$ défini par la condition $x \leq y$. En identifiant $\mathbb{R} \times \mathbb{R}$ avec le plan euclidien à l'aide d'un système de coordonnées, on constate que ce sous-ensemble s'identifie au demi-plan défini par la droite d'équation $y = x$ et qui se trouve au-dessus de cette droite (voir Fig 1).

Exemple 3.12 Soit E un ensemble. La relation d'inclusion sur $\mathcal{P}(E)$ est définie par

$$\subset_E := \{(A, B) \in \mathcal{P}(E) \times \mathcal{P}(E) |\ A \subset B\}.$$

Si E est fixé, on va écrire simplement $\subset$ au lieu de $\subset_E$.

Exercice 3.13 Ecrire explicitement $\subset_E$ pour $E = \{0, 1\}$.

3.2 Propriétés remarquables. Relations d'équivalence et relations d'ordre

On commence par introduire quatre propriétés remarquables portant sur les relations :

Définition 3.14 *Soit A un ensemble. Une relation R sur A est dite*

1. *réflexive, si*
$$\forall x \in A\ (x\ R\ x).$$
2. *transitive, si*
$$\forall x \in A \forall y \in A \forall z \in A\ \big((x\ R\ y) \wedge (y\ R\ z) \Rightarrow (x\ R\ z)\big).$$
3. *symétrique, si*
$$\forall x \in A \forall y \in A\ \big((x\ R\ y) \Rightarrow (y\ R\ x)\big).$$
4. *antisymétrique, si*
$$\forall x \in A \forall y \in A\ \big((x\ R\ y) \wedge (y\ R\ x) \Rightarrow x = y\big).$$

Définition 3.15 *Soit A un ensemble. Une relation R sur A est dite*

1. *relation d'équivalence, si R est réflexive, transitive et symétrique.*
2. *relation d'ordre, si R est réflexive, transitive et antisymétrique.*

Exemples 3.16 1. Soit $\mathcal{G}$ l'ensemble des étudiants de ce groupe (ici présents). La relation

$$R = \{(x, y) |\ x,\ y \text{ sont nés la même année}\}$$

est une relation d'équivalence sur $\mathcal{G}$. Justifier cette affirmation.

2. Soit A un ensemble. La relation d'égalité sur A définie par la diagonale $\Delta_A \subset A \times A$ (voir l'exemple 3.2) est une relation d'équivalence sur A.
3. Soit A un ensemble. Le produit cartésien $\Pi_A := A \times A$ est une relation d'équivalence sur A. Cette relation s'appelle la relation totale sur A.
4. Soit $n \in \mathbb{N}^*$. La relation de congruence mod n est une relation d'équivalence sur $\mathbb{Z}$.
5. Soit $A \subset \mathbb{R}$ un sous-ensemble de $\mathbb{R}$. Le relation sur A définie par la condition $x \leq y$ est une relation d'ordre sur A.
6. La relation de divisibilité sur $\mathbb{N}^*$ est une relation d'ordre sur $\mathbb{N}^*$. Remarquer que la relation de divisibilité sur $\mathbb{Z}$ n'est pas une relation d'ordre sur $\mathbb{Z}$. Pourquoi ?
7. Soit E un ensemble. La relation d'inclusion sur $\mathcal{P}(E)$ est une relation d'ordre sur $\mathcal{P}(E)$.

Soit R une relation d'ordre sur un ensemble A. Un couple $(a, b) \in A \times A$ est dit *R-comparable* (ou on dit que a, b sont des éléments R-comparables) si $a \ R \ b$ ou $b \ R \ a$. Considérons par exemple la relation de divisibilité dans $\mathbb{N}^*$. Les nombres 2, 3 ne sont pas comparables par rapport à la divisibilité parce que $2 \nmid 3$ et $3 \nmid 2$.

Définition 3.17 *Soit A un ensemble. Une relation d'ordre R sur A est dite relation d'ordre total si tout couple $(a, b) \in A \times A$ est R-comparable, i.e. si*

$$\forall (a, b) \in A \times A \ \big((a \ R \ b) \vee (b \ R \ a)\big).$$

Une relation d'ordre qui n'est pas relation d'ordre total s'appelle relation d'ordre partiel[1].

Exemple 3.18 Soit $A \subset \mathbb{R}$ un sous-ensemble de $\mathbb{R}$. La relation sur A définie par la condition $x \leq y$ est une relation d'ordre total sur A. Pourquoi ?

Exemple 3.19 La relation d'ordre sur $\mathbb{N}^*$ définie par la divisibilité est une relation d'ordre qui n'est pas total. Pourquoi ?

Exemple 3.20 Soit E un ensemble qui a deux éléments différents a, b. Alors la relation d'ordre sur $\mathcal{P}(E)$ définie par l'inclusion n'est pas une relation d'ordre total. Pourquoi ? Donner un exemple de deux parties de E (deux éléments de $\mathcal{P}(E)$) qui ne sont pas comparables. Qu'est-ce qu'on peut dire si E est un singleton ?

4 Applications et fonctions

4.1 Définitions

On va utiliser la notation $\exists!$ avec la signification "il existe un unique". Par exemple, d'après la théorie des équations affines étudiée au lycée, nous savons que

$$\forall c \in \mathbb{R} \ \exists! x \in \mathbb{R}, \ 2x = c.$$

Cette proposition nous dit que, pour tout $c \in \mathbb{R}$, l'équation affine $2x = c$ admet une solution *unique* x. Quelle est cette solution ?

Définition 4.1 1. *Une application est un triplet $f = (A, B, R)$ où A, B sont des ensembles et R est une relation entre A et B telle que*

$$\forall x \in A \ \exists! y \in B, \ x \ R \ y.$$

2. *A s'appelle l'ensemble de définition (ou de départ) de f, B s'appelle l'ensemble d'arrivée de f, R s'appelle le graphe de f et sera noté G_f.*
3. *Soit $x \in A$. L'unique élément $y \in B$ tel que $x \ R \ y$ est noté $f(x)$ et s'appelle l'image de x par f. L'ensemble des images par f est un sous-ensemble de B qui est noté $\mathrm{Im}(f)$ et s'appelle l'image de f :*

$$\mathrm{Im}(f) := \{f(x) |\ x \in A\} = \{y \in B |\ \exists x \in A, \ f(x) = y\}.$$

1. En anglais "a partial order relation" signifie une relation d'ordre qui n'est pas *nécessairement* total (mais peut être total).

4. Soit $y \in B$. Un antécédent de y par f est un élément $x \in A$ tel que $f(x) = y$.

Pour préciser que A est l'ensemble de définition, et B est l'ensemble d'arrivée de f on va écrire

$$f : A \to B$$

et on va lire : f est une application définie sur A à valeurs dans B.

Remarque 4.2 Soit $f = (A, B, R)$ une application.

1. Un élément $x \in A$ a une seule image par f, mais un élément $y \in B$ peut avoir un antécédent, plusieurs antécédents, ou n'avoir aucun antécédent.
2. En utilisant la notation $f(x)$ pour l'image de x, nous obtenons la formule suivante pour le graphe G_f de f :
$$G_f = \{(x, f(x))|\ x \in A\}. \tag{1}$$

Deux applications $f_1 = (A_1, B_1, R_1)$, $f_2 = (A_2, B_2, R_2)$ sont égales si et seulement si elles sont égales en tant que triplets, donc si et seulement si $A_1 = A_2$, $B_1 = B_2$ et $R_1 = R_2$, c'est à dire si elles ont les mêmes ensembles de définition, les mêmes ensembles d'arrivée et les mêmes graphes. En utilisant la formule (1) il en résulte

Remarque 4.3 Deux applications $f_1 : A_1 \to B_1$, $f_2 : A_2 \to B_2$ sont égales si et seulement si $A_1 = A_2$, $B_1 = B_2$ et $\forall x \in A_1\ ,\ f_1(x) = f_2(x)$.

La formule (1) montre aussi que, pour définir explicitement une application $f : A \to B$, il suffit de préciser $f(x)$ pour tout $x \in A$.

Exemple 4.4 Soit $f : [0, 6] \to \mathbb{R}$ l'application définie par $f(x) = 2x + 1$. Il s'agit donc du triplet $([0, 6], \mathbb{R}, G_f)$ où $G_f = \{(x, 2x + 1)|\ x \in [0, 6]\}$.

Exemple 4.5 Soit A un ensemble. L'application $f : A \to A$ définie par $f(x) = x$ s'appelle l'application identité de A et est notée id_A. Remarquer que le graphe G_{id_A} de cette application est la diagonale Δ_A du produit cartésien $A \times A$.

Exemple 4.6 Soit A un ensemble, B un ensemble non-vide et soit b un élément de B. L'application constante $f_b : A \to B$ associée à b est définie par $f_b(x) = b$. Remarquer que le graphe G_{f_b} de cette application est

$$\{(x, b)|\ x \in A\} = A \times \{b\}.$$

Définition 4.7 *Soit $f : A \to B$ une application.*

1. *Soit $U \subset A$. La restriction de f à U est l'application $f_{|U} : U \to B$ définie par $f_{|U}(x) = f(x)$ pour tout $x \in U$.*
2. *Soit $V \subset B$ tel que $\mathrm{Im}(f) \subset V$. La restriction au but (ou la corestriction) de f à V est l'application $f^{|V} : A \to V$ définie par $f^{|V}(x) = f(x)$ pour tout $x \in A$.*

Remarquer que le graphe de la restriction $f|_U$ coïncide avec l'intersection $G_f \cap (U \times B)$ et le graphe de la corestriction $f^{|V}$ coïncide avec l'intersection $G_f \cap (A \times V)$. Justifier ces affirmations.

Définition 4.8 *Soit E un ensemble. On appelle suite de E une application $u : \mathbb{N} \to E$. Pour une telle application u on va utiliser la notation u_n au lieu de $u(n)$ et on va écrire $(u_n)_{n\in\mathbb{N}}$ au lieu de $u : \mathbb{N} \to E$.*

Donc la donnée d'une suite de E est équivalente à la donnée, pour tout $n \in \mathbb{N}$, d'un élément $u_n \in E$. On utilise la même terminologie "suite" pour une application $u : \mathbb{N}^* \to E$, ou, plus généralement, pour une application $u : \{n \in \mathbb{N}^*|\ n \geq k\} \to E$. Une telle application sera notée $(u_n)_{n\in\mathbb{N}^*}$, respectivement $(u_n)_{n\geq k}$.

Exemple 4.9 La formule

$$\forall n \in \mathbb{N}^*,\ x_n = \frac{1}{n}$$

définit une suite $(x_n)_{n\in\mathbb{N}^*}$ de $\mathbb{R}$.

4.2 Image directe, image réciproque par une application

Définition 4.10 *Soit $f : A \to B$ une application.*

1. *Soit $A' \subset A$. L'image directe de A' par f est le sous-ensemble $f(A') \subset B$ défini par*

$$f(A') := \{f(x)|\ x \in A'\} = \{y \in B|\ \exists x \in A',\ f(x) = y\}.$$

   En particulier l'image $\mathrm{Im}(f)$ *de f coïncide avec l'image directe $f(A)$.*

2. *Soit $B' \subset B$. L'image réciproque de B' par f est le sous-ensemble $f^{-1}(B') \subset A$ défini par*

$$f^{-1}(B') := \{x \in A|\ f(x) \in B'\}.$$

Dans la notation $f^{-1}(B')$ il ne faut pas essayer de séparer les symboles et les interpréter individuellement ; il ne s'agit pas de l'image directe de B' par une application f^{-1}. On va voir que f^{-1} (l'application réciproque de f) est définie seulement si f est bijective. Par contre l'image réciproque $f^{-1}(B')$ d'un sous-ensemble $B' \subset B$ est définie toujours, sans aucune condition sur f.

Exemple 4.11 Considérons l'application $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2$. Soit $A = [-1, 3]$, $B = [1, 4]$. On a

$$f(A) = \{x^2|\ x \in [-1, 3]\} = \{x^2|\ x \in [-1, 0]\} \cup \{x^2|\ x \in [0, 3]\}.$$

Rappelons que f est strictement décroissante sur $]-\infty, 0]$ et strictement croissante sur $[0, \infty[$. En utilisant ces propriétés, on peut démontrer facilement (par double inclusion) que

$$\{x^2|\ x \in [-1, 0]\} = [0, 1],\ \{x^2|\ x \in [0, 3]\} = [0, 9].$$

Donc $f(A) = [0, 1] \cup [0, 9] = [0, 9]$. Pour l'image réciproque $f^{-1}(B)$ on obtient

$$f^{-1}(B) = \{x \in \mathbb{R}|\ 1 \leq x^2 \leq 4\},$$

donc pour calculer $f^{-1}(B)$ nous devons résoudre le système d'inéquations

$$\begin{cases} x^2 - 1 & \geq & 0 \\ x^2 - 4 & \leq & 0. \end{cases}$$

L'ensemble des solutions de la première inéquation est $]-\infty, -1] \cup [1, \infty[$ et l'ensemble des solutions de la deuxième inéquation est $[-2, 2]$. En calculant l'intersection de ces deux ensembles on obtient

$$f^{-1}(B) = [-2, -1] \cup [1, 2].$$

Proposition 4.12 *(propriétés de l'image directe et de l'image réciproque) Soit $f : A \to B$ une application.*

1. *Pour deux sous-ensembles A_1, $A_2 \subset A$ on a*
   (a) $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.
   (b) $f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2)$.
2. *Soit $A' \subset A$. Alors*
$$A' \subset f^{-1}(f(A')).$$
3. *Soit $B' \subset B$. Alors*
$$f(f^{-1}(B')) = B' \cap \mathrm{Im}(f),$$
   en particulier $f(f^{-1}(B')) \subset B'$.
4. *Pour deux sous-ensembles B_1, $B_2 \subset B$ on a*
   (a) $f^{-1}(B_1 \cup B_2) = f^{-1}(B_1) \cup f^{-1}(B_2)$.
   (b) $f^{-1}(B_1 \cap B_2) = f^{-1}(B_1) \cap f^{-1}(B_2)$.
   (c) $f^{-1}(B_1 \setminus B_2) = f^{-1}(B_1) \setminus f^{-1}(B_2)$.
5. *Soit $B' \subset B$. Notons ${}^cB'$ le complémentaire de B' par rapport à B et ${}^cf^{-1}(B')$ le complémentaire de $f^{-1}(B')$ par rapport à A. On a*
$$f^{-1}({}^cB') = {}^cf^{-1}(B').$$

Démonstration: 3. Démontrons l'égalité $f(f^{-1}(B')) = B' \cap \mathrm{Im}(f)$ pour un sous-ensemble $B' \subset B$.

Pour l'inclusion $f(f^{-1}(B')) \subset B' \cap \mathrm{Im}(f)$:
Soit $y \in f(f^{-1}(B'))$. Par la définition de l'image directe, il existe $x \in f^{-1}(B')$ tel que $f(x) = y$. Par la définition de l'image réciproque, $x \in f^{-1}(B')$ signifie $f(x) \in B'$. Donc $y = f(x) \in B'$. Mais $f(x) \in \mathrm{Im}(f)$ par la définition de $\mathrm{Im}(f)$. Donc $y \in B'$ et $y \in \mathrm{Im}(f)$, donc $y \in B' \cap \mathrm{Im}(f)$.

Pour l'inclusion $B' \cap \mathrm{Im}(f) \subset f(f^{-1}(B'))$:
Soit $y \in B' \cap \mathrm{Im}(f)$. Puisque $y \in \mathrm{Im}(f)$, il existe $x \in A$ tel que $f(x) = y$. Mais aussi $y \in B'$, donc $f(x) = y$ où $y \in B'$. Par la définition de l'image réciproque, $f(x) \in B'$ implique $x \in f^{-1}(B')$. Donc $y = f(x)$ où $x \in f^{-1}(B')$. Par la définition de l'image directe il en résulte $y \in f(f^{-1}(B'))$. ■

Exercice 4.13 Démontrer toutes les affirmations de la proposition 4.12. Pour les égalités utiliser la méthode de la double inclusion.

4.3 Applications injectives, surjectives, bijectives

Définition 4.14 *Une application $f : A \to B$ est dite injective si*

$$\forall x_1 \in A \ \forall x_2 \in A \ (x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)).$$

La condition d'injectivité signifie : les images de deux éléments différents sont toujours différentes. En replaçant l'implication $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ par sa contraposée, on obtient

Remarque 4.15 Une application $f : A \to B$ est injective si et seulement si

$$\forall x_1 \in A \ \forall x_2 \in A \ (f(x_1) = f(x_2) \Rightarrow x_1 = x_2).$$

Définition 4.16 *Une application $f : A \to B$ est dite surjective si*

$$\forall y \in B \ \exists x \in A, \ f(x) = y.$$

La condition de surjectivité signifie : tout élément y de l'ensemble d'arrivée est l'image de (au moins) un élément de l'ensemble de départ, soit : tout élément y de l'ensemble d'arrivée admet (au moins) un antécédent. En tenant compte de la définition de l'image $\mathrm{Im}(f)$ de f on obtient :

Remarque 4.17
1. Une application $f : A \to B$ est surjective si et seulement si $\mathrm{Im}(f) = B$.
2. Soit $f : A \to B$ une application arbitraire. La corestriction (la restriction au but) $f^{|\mathrm{Im}(f)} : A \to \mathrm{Im}(f)$ est surjective.

Définition 4.18 *Une application $f : A \to B$ est dite bijective si elle est injective et surjective.*

En utilisant les définitions de l'injectivité et de la sujectivité on obtient le critère de bijectivité suivant :

Remarque 4.19 Une application $f : A \to B$ est bijective si et seulement si

$$\forall y \in B \ \exists! x \in A, \ f(x) = y.$$

Donc f est bijective si et seulement si *tout* élément $y \in B$ admet un *unique* antécédent.

Exemples 4.20
1. Soit A un ensemble. L'application identique id_A est bijective.
2. Soit $(a, b) \in \mathbb{R}^2$ et $f : \mathbb{R} \to \mathbb{R}$ l'application affine définie par $f(x) = ax + b$. Si $a \neq 0$ cette application est bijective. Si $a = 0$ on obtient l'application constante $f_b : \mathbb{R} \to \mathbb{R}$ qui n'est ni injective, ni surjective.
3. L'application $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = x^2$ n'est ni injective, ni surjective. L'application $g : \mathbb{R} \to [0, \infty[$ définie par la même formule est surjective, mais pas injective. Les restrictions

   $$f_{|[0,\infty[} : [0, \infty[\to \mathbb{R}, \ f_{|]-\infty,0]} :]-\infty, 0] \to \mathbb{R}$$

   de f sont injectives, mais pas surjectives. Les restrictions

   $$g_{|[0,\infty[} : [0, \infty[\to [0, \infty[, \ g_{|]-\infty,0]} :]-\infty, 0] \to [0, \infty[$$

   sont bijectives.

4. L'application $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = e^x$ est injective, mais pas surjective. Par contre, l'application $\exp : \mathbb{R} \to]0, \infty[$ définie par la même formule est bijective.
5. Les applications $\sin : \mathbb{R} \to \mathbb{R}$, $\cos : \mathbb{R} \to \mathbb{R}$ ne sont ni injectives, ni surjectives.
6. Les applications $f : [-\frac{\pi}{2}, \frac{\pi}{2}] \to [-1, 1]$, $g : [0, \pi] \to [-1, 1]$ définies par $f(x) = \sin x$, $g(x) = \cos x$ sont bijectives.
7. L'application $\tan :]-\frac{\pi}{2}, \frac{\pi}{2}[\to \mathbb{R}$ est bijective.

Justifier ces affirmations.

4.4 Composition des applications. Application réciproque

Définition 4.21 *Soient $f : A \to B$, $g : B \to C$ deux applications. La composée $g \circ f$ est l'application $g \circ f : A \to C$ définie par*

$$\forall x \in A \ (g \circ f)(x) := g(f(x)).$$

Voir Fig. 2.

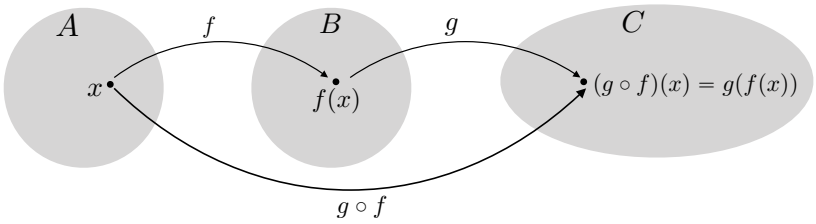


FIGURE 2 – La composée $g \circ f$.

Remarque 4.22 Plus généralement on peut définir la composée $g \circ f$ de deux applications $f : A \to B'$, $g : B'' \to C$ si $\mathrm{Im}(f) \subset B''$. En effet, l'expression $g(f(x))$ est définie si $f(x) \in B''$, donc il suffit de supposer que l'image $\mathrm{Im}(f)$ soit incluse dans le domaine de définition de g. Nous n'avons pas besoin de cette généralisation. En effet, on peut toujours se ramener à la situation considérée dans la définition 4.21 en modifiant l'ensemble d'arrivée de f.

Exemple 4.23 Soient $f : \mathbb{R} \to \mathbb{R}$, $g : \mathbb{R} \to \mathbb{R}$ définies par $f(x) = 2x + 1$, $g(x) = x^2 + 2$. Dans ce cas nous avons $A = B$, donc les deux composées $g \circ f$, $f \circ g$ sont définies. Ces composées sont données par

$$(g \circ f)(x) = g(f(x)) = g(2x + 1) = (2x + 1)^2 + 2 = 4x^2 + 4x + 3,$$

$$(f \circ g)(x) = f(g(x)) = f(x^2 + 2) = 2(x^2 + 2) + 1 = 2x^2 + 5.$$

Cet exemple montre que, en général, pour un ensemble A, la composition des applications $A \to A$ n'est pas une opération commutative.

Remarque 4.24
1. (l'associativité de la composition des applications). Soient $f : A \to B$, $g : B \to C$, $h : C \to D$ trois applications. Alors

$$(h \circ g) \circ f = h \circ (g \circ f).$$

2. (composition avec l'application identité). Soit $f : A \to B$ une application. Alors

$$f \circ \mathrm{id}_A = f, \ \mathrm{id}_B \circ f = f.$$

Démonstration: 1. Les deux composées $(h \circ g) \circ f$, $h \circ (g \circ f)$ sont des applications définies sur le même ensemble A à valeurs dans le même ensemble D. Donc il suffit de de montrer que

$$\forall x \in A \ ((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x).$$

Mais pour tout $x \in A$ on a

$$((h \circ g) \circ f)(x) = (h \circ g)(f(x)) = h(g(f(x))),\ (h \circ (g \circ f))(x) = h((g \circ f)(x)) = h(g(f(x))),$$

donc $((h \circ g) \circ f)(x) = (h \circ (g \circ f))(x)$.

2. Les applications f, $f \circ \mathrm{id}_A$, $\mathrm{id}_B \circ f$ sont définies sur A à valeurs dans B. De plus, pour tout $x \in A$, nous avons :

$$(f \circ \mathrm{id}_A)(x) = f(\mathrm{id}_A(x)) = f(x),\ (\mathrm{id}_B \circ f)(x) = \mathrm{id}_B(f(x)) = f(x).$$

Proposition 4.25 *Soient $f : A \to B$, $g : B \to C$ deux applications.*

1. *Si f et g sont injectives, alors $g \circ f$ est injective.*
2. *Si f et g sont surjectives, alors $g \circ f$ est surjective.*
3. *Si f et g sont bijectives, alors $g \circ f$ est bijective.*
4. *Si $g \circ f$ est injective, alors f est injective.*
5. *Si $g \circ f$ est surjective, alors g est surjective.*

Démonstration: 1. Supposons que f et g sont injectives soient x_1, $x_2 \in A$ tels que $x_1 \neq x_2$. Puisque $x_1 \neq x_2$ et f est injective on a $f(x_1) \neq f(x_2)$. Puisque $f(x_1) \neq f(x_2)$ et g est injective on a $g(f(x_1)) \neq g(f(x_2))$, soit $(g \circ f)(x_1) \neq (g \circ f)(x_2)$.

2. Supposons que f et g sont surjectives. Nous devons démontrer que pour tout $z \in C$ il existe $x \in A$ tel que $(g \circ f)(x) = z$. Soit $z \in C$. Puisque g est surjective, il existe $y \in B$ tel que $g(y) = z$. Puisque f est surjective, il existe $x \in A$ tel que $f(x) = y$. Mais alors $(g \circ f)(x) = g(f(x)) = g(y) = z$. Donc $g \circ f$ est surjective.

3. Résulte de 1. et 2.

4. Supposons que $g \circ f$ est injective et démontrons que f est injective en utilisant la remarque 4.15. Soient x_1, $x_2 \in A$ tels que $f(x_1) = f(x_2)$. En appliquant g on obtient $g(f(x_1)) = g(f(x_2))$, i.e. $(g \circ f)(x_1) = (g \circ f)(x_2)$. Puisque $g \circ f$ est injective, cette égalité implique $x_1 = x_2$. Nous avons démontré l'implication $(f(x_1) = f(x_2)) \Rightarrow (x_1 = x_2)$, donc f est injective.

5. Supposons que $g \circ f$ est surjective. Nous devons démontrer que pour tout $z \in C$ il existe $y \in B$ tel que $g(y) = z$. Soit $z \in C$. Puisque $g \circ f$ est surjective, il existe $x \in A$ tel que $(g \circ f)(x) = z$. On a donc $g(f(x)) = z$. En posant $y := f(x) \in B$ on obtient $g(y) = z$. Donc g est surjective. ■

Définition 4.26 *Soit $f : A \to B$ une application bijective. L'application réciproque $f^{-1} : B \to A$ est définie par*

$$f^{-1}(y) :=\ \textit{l'unique antécédent de } y \textit{ par } f.$$

Donc $f^{-1}(y)$ est l'unique élément $x \in A$ tel que $f(x) = y$.

Exemple 4.27 Soit $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = 2x + 1$. Cette application est bijective. Pourquoi ? Pour déterminer l'application réciproque il faut donner une formule explicite pour $f^{-1}(y)$, c'est à dire résoudre l'équation $f(x) = y$, y étant considéré comme paramètre. L'unique solution de l'équation $2x + 1 = y$ est $x = \frac{1}{2}(y - 1)$. On obtient donc

$$f^{-1}(y) = \frac{1}{2}y - \frac{1}{2}.$$

Pour exprimer l'application réciproque f^{-1} on peut aussi utiliser la variable x. En effet, on n'est pas obligé de désigner par x les éléments de A et par y les éléments de B. Pour un élément $x \in B$, l'image $f^{-1}(x)$ de x par f^{-1} est l'unique élément $y \in A$ tel que $f(y) = x$. Dans l'exemple 4.27 on aura donc

$$f^{-1} : \mathbb{R} \to \mathbb{R},\ f^{-1}(x) = \frac{1}{2}x - \frac{1}{2}.$$

Exemples 4.28 Beaucoup d'applications élémentaires importantes sont définies comme applications réciproques :

1. L'application
$$f : [0, \infty[\to [0, \infty[,\ f(x) = x^2$$
est bijective. Sa réciproque est
$$f^{-1} : [0, \infty[\to [0, \infty[,\ f^{-1}(x) = \sqrt{x}.$$
2. L'application
$$f : \mathbb{R} \to \mathbb{R},\ f(x) = x^3$$
est bijective. Sa réciproque est
$$f^{-1} : \mathbb{R} \to \mathbb{R},\ f^{-1}(x) = \sqrt[3]{x}.$$
3. Plus généralement, pour $n \in \mathbb{N}^*$ pair, l'application
$$f_n : [0, \infty[\to [0, \infty[,\ f_n(x) = x^n$$
est bijective et, pour $n \in \mathbb{N}^*$ impair, l'application
$$f_n : \mathbb{R} \to \mathbb{R},\ f_n(x) = x^n$$
est bijective. On obtient les applications réciproques
$$f_n^{-1} : [0, \infty[\to [0, \infty[,\ f_n^{-1}(x) = \sqrt[n]{x} \text{ si } n \text{ est pair},$$
$$f_n^{-1} : \mathbb{R} \to \mathbb{R},\ f_n^{-1}(x) = \sqrt[n]{x} \text{ si } n \text{ est impair}.$$
4. L'application
$$f : \big[-\frac{\pi}{2}, \frac{\pi}{2} \big] \to [-1, 1],\ f(x) = \sin(x)$$
est bijective. Sa réciproque est l'application
$$\arcsin : [-1, 1] \to \big[-\frac{\pi}{2}, \frac{\pi}{2} \big].$$
5. L'application
$$f : [0, \pi] \to [-1, 1],\ f(x) = \cos(x)$$
est bijective. Sa réciproque est l'application
$$\arccos : [-1, 1] \to [0, \pi].$$
6. L'application
$$f : \big] -\frac{\pi}{2}, \frac{\pi}{2} \big[\to \mathbb{R},\ f(x) = \tan(x)$$
est bijective. Sa réciproque est
$$\arctan : \mathbb{R} \to \big] -\frac{\pi}{2}, \frac{\pi}{2} \big[.$$
7. L'application exponentielle
$$\exp : \mathbb{R} \to]0, \infty[,\ \exp(x) = e^x$$
est bijective. Sa réciproque est l'application
$$\ln :]0, \infty[\to \mathbb{R}.$$

Remarque 4.29 Soit $f : A \to B$ une application bijective et soit f^{-1} la réciproque de f. Alors

1. $f^{-1} \circ f = \mathrm{id}_A$.
2. $f \circ f^{-1} = \mathrm{id}_B$.

Démonstration: 1. Remarquons d'abord que $f^{-1} \circ f$, id_A sont des applications $A \to A$. Pour démontrer que $f^{-1} \circ f = \mathrm{id}_A$ il suffit de montrer que pour tout $x \in A$ on a

$$(f^{-1} \circ f)(x) = x.$$

Mais $(f^{-1} \circ f)(x) = f^{-1}(f(x))$ est (par définition) l'unique antécédent de $f(x)$ donc coïncide avec x.

2. Remarquons d'abord que $f \circ f^{-1}$, id_B sont des applications $B \to B$. Pour démontrer que $f \circ f^{-1} = \mathrm{id}_B$ il suffit de montrer que pour tout $y \in B$ on a

$$(f \circ f^{-1})(y) = y.$$

Mais $f^{-1}(y)$ est (par définition) un antécédent de y, donc $f(f^{-1}(y)) = y$.

■

La remarque suivante montre que les égalités fournies par la remarque 4.29 caractérisent l'application réciproque. Plus précisément

Remarque 4.30 Soit $f : A \to B$ une application. Supposons qu'il existe une application $g : B \to A$ telle que

$$g \circ f = \mathrm{id}_A, \ f \circ g = \mathrm{id}_B. \tag{2}$$

Alors f est bijective et $f^{-1} = g$.

Démonstration: En effet, l'égalité $g \circ f = \mathrm{id}_A$ montre que $g \circ f$ est bijective, en particulier injective, donc, d'après la proposition 4.25.4, il en résulte que f est injective. De manière similaire, l'égalité $f \circ g = \mathrm{id}_B$ montre que f est surjective. Donc f est bijective et l'application réciproque $f^{-1} : B \to A$ existe. Dans (2) composons la première égalité par f^{-1} à droite. On obtient

$$g \circ f = \mathrm{id}_A \Rightarrow (g \circ f) \circ f^{-1} = \mathrm{id}_A \circ f^{-1} \Rightarrow g \circ (f \circ f^{-1}) = f^{-1} \Rightarrow g \circ \mathrm{id}_B = f^{-1} \Rightarrow g = f^{-1}.$$

■

Exemple 4.31 Soit un A ensemble. Une involution sur A est une application $f : A \to A$ telle que $f \circ f = \mathrm{id}_A$. En utilisant la remarque 4.30 il en résulte que toute involution f est bijective et $f^{-1} = f$.

Corollaire 4.32 *Soient $f : A \to B$, $g : B \to C$ deux applications bijectives. Alors*

$$(g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

Démonstration: En utilisant l'associativité de la composition, on remarque que l'application

$$f^{-1} \circ g^{-1} : C \to A$$

a les propriétés

$$(g \circ f) \circ (f^{-1} \circ g^{-1}) = \mathrm{id}_C, \ (f^{-1} \circ g^{-1}) \circ (g \circ f) = \mathrm{id}_A.$$

D'après la remarque 4.30 il en résulte

$$f^{-1} \circ g^{-1} = (g \circ f)^{-1}.$$

■

La remarque suivante est utilisée souvent en combinatoire. Elle intervient implicitement dans la démonstration de la proposition 2.4.

Remarque 4.33 Soit A, B deux ensembles finis. Il existe une application bijective $f : A \to B$ si et seulement si $\mathrm{card}(A) = \mathrm{card}(B)$.

Démonstration: Supposons qu'il existe une bijection $f : A \to B$. Soit $n := \text{card}(A)$, donc on peut "compter" les éléments de A en utilisant les nombres naturels de 1 à n. L'interprétation précise de l'égalité $\text{card}(A) = n$ est donc : il existe une bijection $g : \{1, \ldots, n\} \to A$. Mais alors $f \circ g$ sera une bijection $\{1, \ldots, n\} \to B$ d'après la proposition 4.25. Donc $\text{card}(B) = n = \text{card}(A)$. Réciproquement supposons $\text{card}(A) = \text{card}(B) = n$, donc il existe des bijections $g : \{1, \ldots, n\} \to A$, $h : \{1, \ldots, n\} \to B$. La composée $h \circ g^{-1} : A \to B$ sera bijective. ■

Cette remarque est le point de départ de la théorie des cardinaux pour les ensembles arbitraires (finis ou infinis). En général on dit que deux ensembles A, B (finis ou infinis) *ont le même cardinal* s'il existe une bijection $f : A \to B$.

Proposition 4.34 *Soient A, B deux ensembles finis tels que* $\text{card}(A) = \text{card}(B)$. *Alors*

1. *Toute application injective $f : A \to B$ est bijective.*
2. *Toute application surjective $f : A \to B$ est bijective.*

Démonstration: 1. Soit $f : A \to B$ une application injective. La corestriction $f^{|\text{Im}(f)} : A \to \text{Im}(f)$ est bijective, donc $\text{Im}(f) \subset B$ est un sous-ensemble de B avec $\text{card}(\text{Im}(f)) = \text{card}(A) = \text{card}(B)$. Mais il existe un unique sous-ensemble de B de cardinal maximal $\text{card}(B)$, à savoir B lui-même. Il en résulte $\text{Im}(f) = B$, donc f est bijective.

2. Soit $f : A \to B$ une application surjective. Pour chaque $y \in B$ choisissons un antécédent $x_y \in A$ de y par f. La restriction $f_{|U} : U \to B$ de f au sous-ensemble $U := \{x_y |\ y \in B\}$ est bijective. Pourquoi ? Il en résulté $\text{card}(U) = \text{card}(B) = \text{card}(A)$. Mais il existe un unique sous-ensemble de A de cardinal maximal $\text{card}(A)$, à savoir A lui-même. Il en résulte $U = A$, d'où f est bijective. ■

4.5 Fonctions et correspondances

Une fonction est un triplet (A, B, R) du type considéré dans la définition d'une application, mais c'est une notion plus générale : on requiert seulement l'unicité de l'image d'un élément $x \in A$, pas l'existence. Plus précisément :

Définition 4.35 1. *Une fonction est un triplet $f = (A, B, R)$, où A, B sont des ensembles et R est une relation entre A et B telle que*

$$\forall x \in A\ \forall y \in B\ \forall y' \in B\ \big((x\ R\ y) \wedge (x\ R\ y') \Rightarrow (y = y')\big).$$

Un tel triplet f s'appelle fonction de A vers B, R s'appelle le graphe de f et est noté G_f.

2. *Le domaine de définition d'une fonction f est défini par*

$$D_f := \{x \in A |\ \exists y \in B \text{ tel que } x\ R\ y\}.$$

3. *Soit $x \in D_f$. L'unique élément $y \in B$ tel que $x\ R\ y$ est noté $f(x)$ et s'appelle l'image de x par f.*
4. *Soit $y \in B$. Un antécédent de y par f est un élément $x \in D_f$ tel que $f(x) = y$.*

Le graphe G_f d'une fonction f de A vers B s'écrit

$$G_f = \{(x, f(x)) |\ x \in D_f\}.$$

Donner une fonction f de A vers B revient à préciser :

- Le domaine de définition $D_f \subset A$,
- $f(x) \in B$ pour tout $x \in D_f$.

Exemple 4.36 La formule $f(x) = \frac{x+1}{x-1}$ définit une fonction de $\mathbb{R}$ vers $\mathbb{R}$. Quel est son domaine de définition ? Dessiner son graphe dans le plan euclidien $\mathbb{R}^2$.

Remarque 4.37 1. Une fonction f de A vers B définit une application $f_{\max} : D_f \to B$.

2. La notation $f : A \to B$ signifie que f est *définie* sur A, donc le domaine de définition de f est A. Il s'agit donc d'une application.

3. Dans la littérature mathématique en anglais la notion "function" est utilisée souvent avec une signification différente : "a function" est une application à valeurs dans $\mathbb{R}$ où $\mathbb{C}$.

La *composition* de deux fonctions est définie de la même manière que la composition des applications : Soient f une fonction de A vers B dont le domaine de définition est D_f, et g une fonction de B vers C dont le domaine de définition est D_g. Alors $g \circ f$ est la fonction de A vers C dont le domaine de définition est

$$D_{g\circ f} := \{x \in D_f |\ f(x) \in D_g\}$$

et définie par $(g \circ f)(x) = g(f(x))$ pour tout $x \in D_{g\circ f}$.

Nous concluons ce chapitre avec la définition d'une correspondance. Une correspondance est un triplet du type considéré dans la définition d'une application, mais on n'impose *aucune* condition sur R.

Définition 4.38 *Une correspondance est un triplet $\mathcal{F} = (A, B, R)$, où $R \subset A \times B$ est une relation entre A et B. Un tel triplet s'appelle correspondance de A vers B, R s'appelle le graphe de $\mathcal{F}$ et est noté $G_{\mathcal{F}}$.*

Cette notion très générale dépasse les objectifs de ce cours introductif, donc nous ne l'utiliserons pas dans la suite. Notons seulement qu'une correspondance $\mathcal{F} = (A, B, R)$ définit une application $f_{\mathcal{F}} : A \to \mathcal{P}(B)$ donnée par

$$f_{\mathcal{F}}(x) = \{y \in B |\ x\ R\ y\},$$

donc nous permet d'associer à tout élément $x \in A$ *une partie* de B.

5 Relations d'ordre. Ensembles ordonnés

Soit A un ensemble. Rappelons qu'une relation $R \subset A \times A$ sur A est dite relation d'ordre si R est réflexive, transitive et antisymétrique (voir la définition 3.15). Pour mettre en évidence qu'il s'agit d'une relation d'ordre on va utiliser la notation $a \preccurlyeq b$ au lieu de $a\ R\ b$. Attention à ne pas faire de confusion avec la relation d'ordre usuelle $\leq$ sur $\mathbb{R}$. Il s'agit d'une relation d'ordre arbitraire sur un ensemble arbitraire. La relation d'ordre usuelle sur $\mathbb{R}$ est un cas très particulier de relation d'ordre.

Si $a \preccurlyeq b$, on va dire que a est inférieur à b (au sens de la relation $\preccurlyeq$), ou que b est supérieur à a (au sens de la relation $\preccurlyeq$).

Si $a \preccurlyeq b$ et $a \neq b$ on écrire $a \prec b$ et on va dire que a est *strictement* inférieur à b (au sens de la relation $\preccurlyeq$), ou que b est *strictement* supérieur à a (au sens de la relation $\preccurlyeq$).

Rappelons qu'une relation d'ordre $\preccurlyeq$ sur A est dite relation d'ordre total, si tout couple $(a, b) \in A \times A$ est $\preccurlyeq$ - comparable, i.e. si

$$\forall (a, b) \in A \times A \ \big((a \preccurlyeq b) \vee (b \preccurlyeq a)\big)$$

(voir la définition 3.17).

Définition 5.1 *Un ensemble ordonné est un couple $(A, \preccurlyeq)$, où $\preccurlyeq$ est une relation d'ordre sur A. Un ensemble totalement ordonné est un couple $(A, \preccurlyeq)$, où $\preccurlyeq$ est une relation d'ordre total sur A.*

Remarque 5.2 Soit R une relation d'ordre (total) sur A et soit $B \subset A$. L'intersection $R_B := R \cap (B \times B)$ est une relation d'ordre (total) sur B, qui s'appelle la relation d'ordre *induite* par R sur B. En particulier la relation d'ordre usuelle $\leq$ sur $\mathbb{R}$ induit une relation d'ordre total (désignée par le même symbole) sur tout sous-ensemble $B \subset \mathbb{R}$.

5.1 Plus grand élément, plus petit élément, élément maximal, élément minimal

Définition 5.3 *Soit $(A, \preccurlyeq)$ un ensemble ordonné.*

1. *Un élément $M \in A$ s'appelle plus grand élément (maximum) de A s'il est supérieur à tous les éléments de A, i.e. si*
$$\forall x \in A \ (x \preccurlyeq M).$$
2. *Un élément $m \in A$ s'appelle plus petit élément (minimum) de A s'il est inférieur à tous les éléments de A, i.e. si*
$$\forall x \in A \ (m \preccurlyeq x).$$
3. *Un élément $U \in A$ s'appelle élément maximal de A si dans A il n'existe aucun élément qui lui soit strictement supérieur, i.e. si*
$$\forall x \in A \ (U \preccurlyeq x \Rightarrow x = U).$$
4. *Un élément $u \in A$ s'appelle élément minimal de A si dans A il n'existe aucun élément qui lui soit strictement inférieur, i.e. si*
$$\forall x \in A \ (x \preccurlyeq u \Rightarrow x = u).$$

Proposition 5.4 1. *Si $(A, \preccurlyeq)$ admet un plus grand élément (maximum), il est unique. Plus précisément, si M, $M' \in A$ sont plus grands éléments (maximums), alors $M = M'$.*
2. *Si $(A, \preccurlyeq)$ admet un plus petit élément (minimum), il est unique. Plus précisément, si m, $m' \in A$ sont plus petits éléments (minimums), alors $m = m'$.*
3. *Le plus grand élément de A, s'il existe, est l'unique élément maximal de A.*
4. *Le plus petit élément de A, s'il existe, est l'unique élément minimal de A.*
5. *Si $(A, \preccurlyeq)$ est totalement ordonné, alors tout élément maximal de A est un plus grand élément.*
6. *Si $(A, \preccurlyeq)$ est totalement ordonné, alors tout élément minimal de A est un plus petit élément.*

Démonstration: 1. Soient M, $M' \in A$ plus grands éléments (maximums) de $(A, \preccurlyeq)$. Puisque M est un plus grand élément et $M' \in A$ il en résulte $M' \preccurlyeq M$. Puisque M' est un plus grand élément et $M \in A$ il en résulte $M \preccurlyeq M'$. Donc $M = M'$ par antisymétrie.

2. Argument similaire.

3. Soit M le plus grand élément de A. Pour montrer que M est élément maximal, il faut démontrer que pour tout $x \in A$ avec $M \preccurlyeq x$ on a $x = M$. Soit donc $x \in A$ tel que $M \preccurlyeq x$. Puisque M est le plus grand élément de A on a $x \preccurlyeq M$, donc $x = M$ par antisymétrie. Pour montrer que M est l'unique élément maximal de A, soit U un élément maximal. Puisque M est le plus grand élément de A on a $U \preccurlyeq M$, qui implique $U = M$ par la définition d'un élément maximal.

4. Argument similaire.

5. Supposons que $\preccurlyeq$ est une relation d'ordre total et soit $U \in A$ un élément maximal. Pour montrer que U est un plus grand élément de A soit $x \in A$. L'ordre $\preccurlyeq$ est total, donc $U \preccurlyeq x$ ou $x \preccurlyeq U$. Puisque U est maximal, dans le premier cas on obtient $x = U$, qui est un cas particulier du deuxième cas $x \preccurlyeq U$. Donc on a toujours $x \preccurlyeq U$, qui montre que U est un maximum.

6. Argument similaire. ■

Proposition 5.5 *Soit $(A, \preccurlyeq)$ un ensemble totalement ordonné fini et non-vide. Alors le plus petit élément (le minimum) et le plus grand élément (le maximum) de A existent.*

Démonstration: Récurrence par rapport à $n := \mathrm{card}(A)$. L'affirmation est évidente pour $n = 1$. Supposons qu'elle vraie pour tout ensemble totalement ordonné de cardinal n et soit $(A, \preccurlyeq)$ un ensemble totalement ordonné de cardinal $n + 1$. Puisque l'ordre $\preccurlyeq$ est total, $\max\{a, b\}$ existe pour tout couple $(a, b) \in A \times A$. Choisissons $a \in A$. Il suffit de remarquer que $\mathrm{card}(A \setminus \{a\}) = n$ et $\max\{a, \max(A \setminus \{a\})\}$ est un plus grand élément de A. ■

L'affirmation n'est *pas* vraie sans supposer que A est muni d'un ordre *total*.

Exemples 5.6

1. Le minimum de l'ensemble ordonné $(\mathbb{N}, \leq)$ est 0, mais cet ensemble n'a pas de maximum.
2. L'ensemble ordonné $(\mathbb{Z}, \leq)$ n'a ni maximum, ni minimum.
3. Le maximum (minimum) de l'ensemble ordonné $([0, 1], \leq)$ est 1 (respectivement 0). Démontrer ces affirmations.
4. Le maximum de l'ensemble ordonné $]0, 1] \subset \mathbb{R}$ est 1, mais cet ensemble n'a pas de minimum. Démontrer ces affirmations.
5. Soit E un ensemble et soit $(\mathcal{P}(E), \subset)$ l'ensemble des parties de E ordonné par l'inclusion (voir l'exemple 3.12). Le maximum de $\mathcal{P}(E)$ est E et le minimum de $\mathcal{P}(E)$ est $\emptyset$.
6. Soit $E = \{1, 2, 3\}$ et soit $(\mathcal{P}(E) \setminus \{\emptyset\}, \subset)$ l'ensemble des parties non-vides de E, ordonné par l'inclusion. Le maximum de $\mathcal{P}(E) \setminus \{\emptyset\}$ est E, mais $\mathcal{P}(E) \setminus \{\emptyset\}$ n'a pas de minimum. Par contre $\mathcal{P}(E) \setminus \{\emptyset\}$ admet trois éléments minimaux, à savoir $\{1\}$, $\{2\}$, $\{3\}$. Démontrer ces affirmations.
7. Plus généralement, soit E un ensemble non-vide et soit $(\mathcal{P}(E) \setminus \{\emptyset\}, \subset)$ l'ensemble des parties non-vides de E, ordonné par l'inclusion. Quels sont les éléments minimaux de cet ensemble ordonné ?
8. Soit $E = \{1, 2, 3\}$ et soit $(\mathcal{P}(E) \setminus \{E\}, \subset)$ l'ensemble des parties $A \subsetneq E$, ordonné par l'inclusion. Le minimum de $\mathcal{P}(E) \setminus \{E\}$ est $\emptyset$, mais $\mathcal{P}(E) \setminus \{E\}$ n'a pas de maximum. Par contre $\mathcal{P}(E) \setminus \{E\}$ admet trois éléments maximaux, à savoir $\{1, 2\}$, $\{2, 3\}$, $\{1, 3\}$. Démontrer ces affirmations et généraliser cet énoncé pour un ensemble E non-vide.
9. Soit $\mathbb{N}^*$ ordonné par la relation de divisibilité. Le minimum de cet ensemble est 1, mais cet ensemble n'a pas de maximum. Remarquer aussi que cet ensemble n'admet aucun élément maximal. Pourquoi ?
10. Soit $\mathbb{N}$ ordonné par la relation de divisibilité : $a|b$ s'il existe $q \in \mathbb{N}$ tel que $b = aq$. Dans cet ensemble ordonné 0 est le *plus grand* élément. En effet, pour tout $a \in \mathbb{N}$ on évidemment $a|0$. Donc 0 est le *maximum* de ensemble ordonné $(\mathbb{N}, |)$, bien que le même élémént est le *minimum* de l'ensemble ordonné $(\mathbb{N}, \leq)$.
11. Soit $\mathbb{N}^* \setminus \{1\}$ ordonné par la relation de divisibilité. Cet ensemble n'admet pas de minimum, mais il admet des éléments minimaux. Quels sont les éléments minimaux de $\mathbb{N}^* \setminus \{1\}$ par rapport à la relation de divisibilité ?

12. Soit $E := \{x \in \mathbb{N}^* |\ 2 \leq x \leq 100\}$ ordonné par la relation de divisibilité. Cet ensemble n'admet aucun minimum et aucun maximum. Pourquoi ? Quels sont les éléments minimaux de $(E, |)$? Quels sont les éléments maximaux de $(E, |)$?

5.2 Sous-ensembles de $\mathbb{N}$

Une propriété fondamentale de l'ensemble totalement ordonné $(\mathbb{N}, \leq)$ est :

Théorème 5.7 *Tout sous-ensemble non-vide $B \subset \mathbb{N}$ admet un plus petit élément.*

On va omettre la démonstration. On peut démontrer ce théorème soit en utilisant la propriété de la borne supérieure de l'ensemble ordonnée $(\mathbb{R}, \leq)$ (voir la section 5.4), soit en restant dans le cadre de la théorie des nombres naturels en utilisant les axiomes de Péano :

`https://fr.wikipedia.org/wiki/Axiomes_de_Peano`.

Si on utilise la première méthode on peut déduire le résultat suivant (qui figure comme axiome dans la théorie de Péano) et sur lequel s'appuie le principe de démonstration par recurrence.

Proposition 5.8 *Soit $B \subset \mathbb{N}$ un sous-ensemble tel que*

1. $0 \in B$,
2. $\forall n \in \mathbb{N}\ (n \in B \Rightarrow n + 1 \in B)$.

Alors $B = \mathbb{N}$.

La deuxième condition signifie : si un naturel n appartient à B, alors aussi son *successeur* $n+1$ appartient à B.

Démonstration: (en admettant le théorème 5.7) Supposons, par l'absurde $B \neq \mathbb{N}$. Alors $C := \mathbb{N} \setminus B \neq \emptyset$, donc d'après le théorème 5.7 le plus petit élément m de C existe. On ne peut pas avoir $m = 0$, parce que $0 \in B$ par hypothèse. Donc $m > 0$ et $m - 1 \in \mathbb{N}$. Puisque m est élément minimal de C il en résulte $m - 1 \notin C$, donc $m - 1 \in B$. Mais alors la deuxième hypothèse nous donne $m = (m - 1) + 1 \in B$, ce qui contredit $m \in C$. ■

Notons que tout sous-ensemble *fini* et non-vide de $\mathbb{R}$ (en particulier de $\mathbb{N}$) admet un plus grand élément et un plus petit élément. C'est un cas particulier de la proposition 5.5.

5.3 Majorants, minorants, borne supérieure, borne inférieure

Les notions de plus petit élément, plus grand élément, élément minimal, élément maximal introduites ci-dessus concernent un ensemble ordonné. S'il existe, un plus grand élément (un plus petit élément, un élément maximal, un élément minimal) d'un ensemble ordonné $(B, \preccurlyeq)$ est toujours un élément de B.

Les notions de majorant, minorant, borne supérieure, borne inférieure qu'on va introduire ci-dessous, concernent *un sous-ensemble* B d'un ensemble ordonné $(A, \preccurlyeq)$. S'il existe, un majorant (un minorant, une borne supérieure, une borne inférieure) d'un sous-ensemble $B \subset A$ est un élément de A, mais *pas* nécessairement élément de B.

Définition 5.9 *Soit $(A, \preccurlyeq)$ un ensemble ordonné et soit $B \subset A$.*

1. *Un majorant de B dans A est un élément $\mu \in A$ tel que*

$$\forall x \in B\ (x \preccurlyeq \mu).$$

2. *Un minorant de B dans A est un élément $\nu \in A$ tel que*

$$\forall x \in B\ (\nu \preccurlyeq x).$$

3. *Soient $\mathcal{M}\mathrm{aj}(B) \subset A$ l'ensemble des majorants de B et $\mathcal{M}\mathrm{in}(B) \subset A$ l'ensemble des minorants de B. B est dit sous-ensemble majoré s'il admet (au moins) un majorant, donc si $\mathcal{M}\mathrm{aj}(B) \neq \emptyset$. B est dit sous-ensemble minoré s'il admet (au moins) un minorant, donc si $\mathcal{M}\mathrm{in}(B) \neq \emptyset$. B est dit sous-ensemble borné s'il est majoré et minoré.*

4. *Supposons que B est majoré. Le minimum de $\mathcal{M}\mathrm{aj}(B)$, s'il existe, s'appelle la borne supérieure de B et est noté* $\sup(B)$.
5. *Supposons que B est minoré. Le maximum de $\mathcal{M}\mathrm{in}(B)$, s'il existe, s'appelle la borne inférieure de B et est noté* $\inf(B)$.

Dire que $\mu \in A$ est la borne supérieure de B, signifie que μ est un majorant de B et μ est le plus petit majorant de B. Si $\preccurlyeq$ est une relation d'ordre total, la deuxième condition est équivalente à "μ est un élément minimal dans l'ensemble des majorants de B", qui peut être reformulée de la manière suivante : tout élément $x \prec \mu$ n'est plus un majorant de B, c'est à dire : pour tout élément $x \prec \mu$ il existe un élément $b \in B$ tel que $x \prec b$. On obtient donc la caractérisation suivante de la borne supérieure (inférieure) d'un sous-ensemble d'un ensemble totalement ordonné :

Proposition 5.10 *Soient $(A, \preccurlyeq)$ un ensemble totalement ordonné et $B \subset A$ un sous-ensemble de A.*

1. *Soit $\mu \in A$. Alors $\mu = \sup(B)$ si et seulement si*
   (a) *μ est un majorant de B et*
   (b) *$\forall x \in A\ (x \prec \mu \Rightarrow \exists b \in B,\ x \prec b \preccurlyeq \mu)$.*
2. *Soit $\nu \in A$. Alors $\nu = \inf(B)$ si et seulement si*
   (a) *ν est un minorant de B et*
   (b) *$\forall x \in A\ (\nu \prec x \Rightarrow \exists b \in B,\ \nu \preccurlyeq b \prec x)$.*

Exemple 5.11 Un sous-ensemble $B \subset \mathbb{Z}$ est borné par rapport à l'ordre usuel $\leq$ si et seulement s'il est fini. Si c'est le cas et $B \neq \emptyset$, le plus grand élément et le plus petit élément de B existent d'après la proposition 5.5.

Exemple 5.12 Soit $(A, \preccurlyeq)$ un ensemble ordonné et soit $B \subset A$ un sous-ensemble muni de la relation d'ordre induite. Si le plus grand élément M de B existe, alors $\sup(B) = M$. Si le plus petit élément m de B existe, alors $\inf(B) = m$.

Exemple 5.13 Soit $A = \mathbb{R}$ muni de la relation d'ordre usuelle et soit $B =]0, 1[$. L'ensemble $\mathcal{M}\mathrm{aj}(B)$ des majorants de B est $[1, \infty[$. Le minimum de cet ensemble est 1, donc $\sup(]0, 1[) = 1$. L'ensemble $\mathcal{M}\mathrm{in}(B)$ des minorants de B est $]-\infty, 0]$. Le maximum de cet ensemble est 0, donc $\inf(]0, 1[) = 0$.

Exemple 5.14 Soit $A = \mathbb{R}$ muni de la relation d'ordre usuelle et soit $B = \left\{ \frac{1}{10^n} |\ n \in \mathbb{N} \right\}$. On a $\mathcal{M}\mathrm{aj}(B) = [1, \infty[$, $\mathcal{M}\mathrm{in}(B) =]-\infty, 0]$, $\sup(B) = 1$, $\inf(B) = 0$. Démontrer ces affirmations.

5.4 La densité de $\mathbb{Q}$ dans $\mathbb{R}$. La propriété de la borne supérieure de $\mathbb{R}$

On va commencer par une propriété importante : la densité de $\mathbb{Q}$ dans l'ensemble ordonné $(\mathbb{R}, \leq)$:

Proposition 5.15 *(la densité de $\mathbb{Q}$ dans $\mathbb{R}$) Soient x, $y \in \mathbb{R}$ tels que $x < y$. Alors il existe $q \in \mathbb{Q}$ tel que*

$$x < q < y.$$

Démonstration: Puisque $y - x > 0$, il existe $n \in \mathbb{N}$ tel que $\frac{1}{10^n} < y - x$ (voir l'exemple 5.14). Soit $q_n := \frac{[10^n x]}{10^n}$ l'approximation décimale de x par défaut à 10^{-n}. On a donc

$$q_n \leq x < q_n + \frac{1}{10^n}.$$

En posant $q = q_n + \frac{1}{10^n} \in \mathbb{Q}$, on a bien $x < q < y$. En effet, la première inégalité est connue et la deuxième résulte de

$$q = x + (q - x) \leq x + (q - q_n) = x + \frac{1}{10^n} < x + (y - x) = y.$$

■

Voici un exemple intéressant (un calcul de borne supérieure) qui utilise la propriété de densité de $\mathbb{Q}$:

Exemple 5.16 Considérons le sous-ensemble $B \subset \mathbb{R}$ défini par

$$B := \{q \in \mathbb{Q}_+ |\ q^2 < 2\} = [0, \sqrt{2}[\cap\mathbb{Q}.$$

Nous avons $\sup(B) = \sqrt{2}$.

Démonstration: En effet $\sqrt{2}$ est bien un majorant de B. D'après la proposition 5.10, il suffit de montrer que pour tout $x \in \mathbb{R}$ tel que $x < \sqrt{2}$, il existe $q \in B$ tel que $x < q$. Soit donc $x < \sqrt{2}$. Remarquer que $\max\{0, x\} < \sqrt{2}$, donc, d'après la propriété de densité de $\mathbb{Q}$ dans $\mathbb{R}$, il existe $q \in \mathbb{Q}$ tel que

$$\max\{0, x\} < q < \sqrt{2}.$$

Avec ce choix on a bien $q \in B$ et $x < q$. ■

Définition 5.17 *Soit $(A, \preccurlyeq)$ un ensemble ordonné. On dit que $(A, \preccurlyeq)$ a la propriété de la borne supérieure si pour tout sous-ensemble non-vide et majoré $B \subset A$ la borne supérieure* $\sup(B)$ *existe.*

Proposition 5.18 *L'ensemble ordonné $(\mathbb{Q}, \leq)$ n'a pas la propriété de la borne supérieure.*

Démonstration: En effet considérons l'ensemble

$$B := \{q \in \mathbb{Q}_+ |\ q^2 < 2\} = [0, \sqrt{2}[\cap\mathbb{Q}$$

étudié dans l'exemple 5.16. Ce sous-ensemble de $\mathbb{Q}$ est non-vide et majoré. On va montrer que B n'admet pas de borne supérieure *dans* $\mathbb{Q}$.

En effet, nous savons que, si on regarde B comme sous-ensemble de $\mathbb{R}$, on aura $\sup(B) = \sqrt{2}$. L'ensemble des majorants de cet ensemble *dans* $\mathbb{R}$ est donc $[\sqrt{2}, \infty[$. L'ensemble des majorants de B *dans* $\mathbb{Q}$ sera $[\sqrt{2}, \infty[\cap\mathbb{Q}$. Mais, puisque $\sqrt{2} \notin \mathbb{Q}$, on a $[\sqrt{2}, \infty[\cap\mathbb{Q} =]\sqrt{2}, \infty[\cap\mathbb{Q}$. En utilisant de nouveau la propriété de densité de $\mathbb{Q}$, on constate facilement (par l'absurde) que ce sous-ensemble de $\mathbb{Q}$ n'admet pas de minimum. ■

Un théorème fondamental de l'analyse affirme :

Théorème 5.19 *Pour tout sous-ensemble non-vide et majoré B de $\mathbb{R}$ (muni de l'ordre standard), la borne supérieure* $\sup(B)$ *existe.*

Autrement dit, *l'ensemble ordonné $(\mathbb{R}, \leq)$ a la propriété de la borne supérieure*. Notons que l'ensemble $\mathbb{R}$ des nombres réels peut être introduit par une approche axiomatique et dans l'une des théories axiomatiques des nombres réels *cette propriété est un axiome, pas un théorème* :

`https://fr.wikipedia.org/wiki/Nombre_réel#Approche_axiomatique`.

En utilisant la bijection $x \mapsto -x$ (la symétrie de la droite réelle par rapport à l'origine) on déduit facilement :

Corollaire 5.20 *Pour tout sous-ensemble non-vide et minoré B de $\mathbb{R}$ la borne inférieure* $\inf(B)$ *existe.*

Démonstration: Soit $B \subset \mathbb{R}$ un sous-ensemble non-vide minoré. Le sous-ensemble $-B := \{-b |\ b \in B\}$ est non-vide et majoré, donc $\sup(-B)$ existe d'après le théorème 5.19. C'est facile de vérifier que $-\sup(-B)$ est la borne inférieure de B. ■

5.5 Ensembles ordonnés remarquables

5.5.1 Les sous-ensembles de $\mathbb{R}$

Les premiers exemples importants d'ensembles ordonnés sont les sous-ensembles de $\mathbb{R}$ (voir la remarque 5.2). Pour tout $B \subset \mathbb{R}$ on obtient un ensemble totalement ordonné $(B, \leq)$ obtenu en munissant B de la relation d'ordre total induite sur B par la relation usuelle $\leq$ sur $\mathbb{R}$. Pour simplifier les notations, nous avons utilisé la même notation $\leq$ pour la relation induite sur B, mais certains auteurs utilisent la notation plus précise $\leq_B$.

En particulier, les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ (qui sont des sous-ensembles de $\mathbb{R}$) et tout intervalle $I \subset \mathbb{R}$ sont munis naturellement d'une relation d'ordre total.

5.5.2 L'ensemble ordonné $(\mathcal{P}(E), \subset)$

Nous avons vu que l'ensemble des parties $\mathcal{P}(E)$ muni de l'inclusion est un ensemble ordonné. Si E contient deux éléments différents, alors cet ordre est partiel (pas total). En effet, si $a \neq b$, alors $\{a\} \not\subset \{b\}$ et $\{b\} \not\subset \{a\}$.

Bien évidemment, tout sous-ensemble de $\mathcal{P}(E)$ sera muni naturellement d'une relation d'ordre induite. Par exemple $(\mathcal{P}(E)\setminus\{\emptyset\}, \subset)$ est un ensemble ordonné. Cet ensemble ordonné admet des éléments minimaux : si $E \neq \emptyset$, les éléments minimaux de $(\mathcal{P}(E) \setminus \{\emptyset\}, \subset)$ sont les singletons $\{x\}$, $x \in E$. Si E contient deux éléments distincts, l'ensemble ordonné $(\mathcal{P}(E) \setminus \{\emptyset\}, \subset)$ n'admet pas de minimum.

5.5.3 L'ensemble ordonné $(\mathbb{N}^*, |)$, pgcd et pppcm

La divisibilité définit une relation d'ordre notée $|$ sur $\mathbb{N}^*$. C'est une relation d'ordre partiel (pas total). En effet $2 \nmid 3$ et $3 \nmid 2$.

Remarque 5.21 Soit $B \subset \mathbb{N}^*$. Sont équivalentes :

1. B est majoré par rapport à la relation d'ordre total $\leq$.
2. B est majoré par rapport à la relation d'ordre partiel $|$.
3. B est fini.

Démonstration: L'équivalence 1. $\Leftrightarrow$ 3. est évidente (voir l'exemple 5.11). Pour l'implication 2. $\Rightarrow$ 3. : on utilise la factorisation des nombres naturels non-nuls en produit de facteurs premiers pour montrer que l'ensemble des diviseurs d'un nombre $N \in \mathbb{N}^*$ est fini. Pour l'implication 3. $\Rightarrow$ 2. : notons que, pour un ensemble fini $B \subset \mathbb{N}^*$, le produit $\Pi_{b\in B} b$ est un multiple commun des éléments de B, donc un majorant de B par rapport à l'ordre $|$. ■

Soit $(m, n) \in \mathbb{N}^* \times \mathbb{N}^*$ un couple de nombres naturels non-nuls. Le sous-ensemble $\{k \in \mathbb{N}^* |\ k|m \text{ et } k|n\} \subset \mathbb{N}^*$ est non-vide et majoré (donc fini) ; le sous-ensemble $\{N \in \mathbb{N}^* |\ m|N \text{ et } n|N\} \subset \mathbb{N}^*$ est non-vide. En utilisant la proposition 5.5 et le théorème 5.7 il en résulte que le maximum $\max\left\{k \in \mathbb{N}^* |\ k|m \text{ et } k|n\right\}$ et le minimum $\min\left\{N \in \mathbb{N}^* |\ m|N \text{ et } n|N\right\}$ (par rapport à la relation d'ordre usuelle $\leq$) existent.

Définition 5.22 *Le plus grand commun diviseur (le* pgcd*) et le plus petit commun multiple (le* ppcm*) de* $(m, n) \in \mathbb{N}^* \times \mathbb{N}^*$ *sont définis par*

$$\mathrm{pgcd}(m, n) := \max\left\{k \in \mathbb{N}^* |\ k|m \text{ et } k|n\right\},\ \mathrm{ppcm}(m, n) := \min\left\{N \in \mathbb{N}^* |\ m|N \text{ et } n|N\right\}. \tag{3}$$

La proposition suivante affirme que tout diviseur commun de m et n est un diviseur de $\mathrm{pgcd}(m, n)$ et tout multiple commun de m et n est un multiple de $\mathrm{ppcm}(m, n)$. Autrement dit : $\mathrm{pgcd}(m, n)$ est la borne inférieure de $\{m, n\}$ et $\mathrm{ppcm}(m, n)$ est la borne supérieure de $\{m, n\}$ *par rapport à la relation de divisibilité* :

Proposition 5.23 *Soient* m, n *éléments de* $\mathbb{N}^*$.

1. *Soit* $\mu \in \mathbb{N}^*$ *un multiple commun de* m *et* n. *Alors* $\mathrm{ppcm}(m, n)|\mu$.
2. *Soit* $\delta \in \mathbb{N}^*$ *un diviseur commun de* m *et* n. *Alors* $\delta|\mathrm{pgcd}(m, n)$.

Démonstration: 1. Soient q, r le quotient, respectivement le reste de la division euclidienne de μ par $\mathrm{ppcm}(m, n)$ (voir le théorème 3.5). On a donc $0 \leq r < \mathrm{ppcm}(m, n)$. Supposons par l'absurde que $\mathrm{ppcm}(m, n)$ ne divise pas μ. Alors on aura $r \in \mathbb{N}^*$ et $r = \mu - q \cdot \mathrm{ppcm}(m, n)$ sera un multiple commun de m et n strictement positif et strictement plus petit que $\mathrm{ppcm}(m, n)$. Ceci contredit la définition de $\mathrm{ppcm}(m, n)$.

2. Remarquer que m, n sont des multiples communs de $d := \mathrm{pgcd}(m, n)$ et δ. En utilisant 1. on obtient $\mathrm{ppcm}(d, \delta)|m$ et $\mathrm{ppcm}(d, \delta)|n$, donc $\mathrm{ppcm}(d, \delta)$ est un diviseur commun de m et n. Mais évidemment $\mathrm{ppcm}(d, \delta) \geq d$ et $d := \mathrm{pgcd}(m, n)$ est le diviseur commun *maximal* de m et n, donc $\mathrm{ppcm}(d, \delta) = d$, donc $d = \mathrm{pgcd}(m, n)$ est un multiple de δ. ■

Rappelons la méthode de calcul des pgcd, ppcm de deux nombres $m, n \in \mathbb{N}^*$: Soit $\{p_1, \ldots, p_k\}$ l'ensemble (écrit sans répétitions) des nombres premiers qui interviennent dans les factorisations en produit des nombres

premiers de m et n. On a donc

$$m = \prod_{i=1}^{k} p_i^{a_i},\ n = \prod_{i=1}^{k} p_i^{b_i} \text{ avec } a_i,\ b_i \in \mathbb{N}.$$

Alors

$$\text{pgcd}(m,n) = \prod_{i=1}^{k} p_i^{\min(a_i,b_i)},\ \text{ppcm}(m,n) = \prod_{i=1}^{k} p_i^{\max(a_i,b_i)}. \tag{4}$$

Les notions pgcd, ppcm et les formules de calcul (4) se généralisent facilement pour un l-uplet $(n_1, \ldots, n_l)$ de nombres naturels non-nuls. Il en résulte :

Proposition 5.24 *Toute partie finie non-vide $B \subset \mathbb{N}^*$ admet une borne supérieure et une borne inférieure par rapport à la relation d'ordre $|$. La borne inférieure (supérieure) de B par rapport à cette relation d'ordre coïncide avec le* pgcd *(respectivement* ppcm*) des éléments de B.*

Exercice 5.25 Démontrer l'identité $\text{pgcd}(m,n)\text{ppcm}(m,n) = mn$. Utiliser (4) et l'identité

$$\min(x,y) + \max(x,y) = x + y.$$

Remarque 5.26 La divisibilité définit aussi une relation d'ordre sur $\mathbb{N}$. Rappelons que 0 est le plus grand élément de l'ensemble ordonné $(\mathbb{N}, |)$ (voir les exemples 5.6). Pour tout couple $(a,b) \in \mathbb{N} \times \mathbb{N}$ la borne inférieure $\inf_|\{a,b\}$ et la borne supérieure $\sup_|\{a,b\}$ par rapport à la relation de divisibilité existent et sont données par :

$$\inf\nolimits_|\{a,b\} = \begin{cases} \text{pgcd}(a,b) & \text{si} \quad (a \neq 0) \wedge (b \neq 0) \\ a & \text{si} \quad (a \neq 0) \wedge (b = 0) \\ b & \text{si} \quad (a = 0) \wedge (b \neq 0) \\ 0 & \text{si} \quad a = b = 0 \end{cases}, \quad \sup\nolimits_|\{a,b\} = \begin{cases} \text{ppcm}(a,b) & \text{si} \quad (a \neq 0) \wedge (b \neq 0) \\ 0 & \text{si} \quad (a = 0) \vee (b = 0) \end{cases}.$$

On peut désigner $\inf_|\{a,b\}$ par $\text{pgcd}(a,b)$ et $\sup_|\{a,b\}$ par $\text{ppcm}(a,b)$ pour tout couple $(a,b) \in \mathbb{N} \times \mathbb{N}$. Remarquer quand même que $0 = \inf_|\{0,0\}$ n'est pas "le plus grand" diviseur commun de 0 et 0 au sens de la relation d'ordre total $\leq$, mais seulement au sens de la relation de divisibilité (comparer avec la définition 5.22).

5.5.4 Ensembles d'applications à valeurs dans un ensemble ordonné

Soit A un ensemble, $(B, \trianglelefteq)$ un ensemble ordonné et soit

$$\mathcal{F}(A,B) := \{f |\ f : A \to B \text{ application}\}$$

l'ensemble des applications définies sur A à valeurs dans B. Cet ensemble peut être muni naturellement d'une relation d'ordre définie par

$$f \trianglelefteq g \text{ si } \forall x \in A,\ f(x) \trianglelefteq g(x).$$

Dans le cas particulier $(B, \trianglelefteq) = (\mathbb{R}, \leq)$ cette relation d'ordre sur l'ensemble des applications $A \to \mathbb{R}$ joue un rôle très important en analyse. Notons que, en général, $(\mathcal{F}(A,B), \trianglelefteq)$ n'est pas totalement ordonné, même si $(B, \trianglelefteq)$ est totalement ordonné.

Exemple 5.27 Soient $f, g : \mathbb{R} \to \mathbb{R}$ les applications définies par $f(x) = x$, $g(x) = -x$. L'ensemble d'arrivée $\mathbb{R}$ est muni de la relation d'ordre total usuelle. Puisque $f(-1) < g(-1)$ on a $g \not\trianglelefteq f$. Puisque $g(1) < f(1)$ on a $f \not\trianglelefteq g$. Donc les applications f, g ne sont pas comparables par rapport à la relation $\leq$ sur $\mathcal{F}(\mathbb{R}, \mathbb{R})$.

5.6 Applications et relations d'ordre

Définition 5.28 *Soit A un ensemble et soit $(B, \trianglelefteq)$ un ensemble ordonné. Une application $f : A \to B$ est dite*

1. *majorée, si le sous-ensemble* $\text{Im}(f) \subset B$ *est majoré.*
2. *minorée, si le sous-ensemble* $\text{Im}(f) \subset B$ *est minoré.*

3. bornée, si le sous-ensemble $\mathrm{Im}(f) \subset B$ *est borné.*

Pour un sous-ensemble $A' \subset A$ *on va dire que* f *est majorée (minorée, bornée) sur* A' *si la restriction* $f_{|A'}$ *est majorée (respectivement minorée, bornée).*

Donc

1. f est majorée si et seulement si il existe $\mu \in B$ tel que $f(x) \trianglelefteq \mu$ pour tout $x \in A$. Un tel élément $\mu \in B$ s'appelle majorant de f.
2. f est minorée si et seulement si il existe $\nu \in B$ tel que $\nu \trianglelefteq f(x)$ pour tout $x \in A$. Un tel élément $\nu \in B$ s'appelle minorant de f.
3. f est bornée si et seulement si il existe $(\nu, \mu) \in B \times B$ tel que $\nu \trianglelefteq f(x) \trianglelefteq \mu$ pour tout $x \in A$.

Exemples 5.29 1. L'application affine

$$f : \mathbb{R} \to \mathbb{R},\ f(x) = 2x + 1$$

n'est ni majorée, ni minorée, mais elle est bornée sur tout intervalle $[a, b]$ avec $a \leq b$.

2. Les applications $\cos : \mathbb{R} \to \mathbb{R}$, $\sin : \mathbb{R} \to \mathbb{R}$ sont bornées.
3. L'application

$$f :]0, \infty[\to \mathbb{R},\ f(x) = \frac{1}{x}$$

est minorée, mais pas majorée.

Soit $f : A \to B$ une application et soit $A' \subset A$. La borne supérieure (inférieure) de f sur A' est définie par

$$\sup_{x \in A'} f(x) := \sup\{f(x) |\ x \in A'\}\ (\inf_{x \in A'} f(x) := \inf\{f(x) |\ x \in A'\})$$

si cette borne supérieure (respectivement inférieure) existe.

Le théorème 5.19 et le corollaire 5.20 montrent que :

Remarque 5.30 Supposons $(B, \trianglelefteq) = (\mathbb{R}, \leq)$, soit $f : A \to \mathbb{R}$ une application et soit $A' \subset A$.

1. si $A' \neq \emptyset$ et f est majoré sur A', alors la limité supérieure $\sup_{x \in A'} f(x)$ existe.
2. si $A' \neq \emptyset$ et f est minoré sur A', alors la limité inférieure $\inf_{x \in A'} f(x)$ existe.

Définition 5.31 *Soient* $(A, \preccurlyeq)$, $(B, \trianglelefteq)$ *ensembles ordonnés. Une application* $f : A \to B$ *est dite*

1. croissante, si

$$\forall x \in A\ \forall x' \in A\ (x \preccurlyeq x' \Rightarrow f(x) \trianglelefteq f(x')).$$

2. décroissante, si

$$\forall x \in A\ \forall x' \in A\ (x \preccurlyeq x' \Rightarrow f(x') \trianglelefteq f(x)).$$

3. monotone, si f *est croissante ou décroissante.*

4. strictement croissante, si

$$\forall x \in A\ \forall x' \in A\ (x \prec x' \Rightarrow f(x) \triangleleft f(x')).$$

5. strictement décroissante, si

$$\forall x \in A\ \forall x' \in A\ (x \prec x' \Rightarrow f(x') \triangleleft f(x)).$$

6. strictement monotone, si f *est strictement croissante ou strictement décroissante.*

Dans cette définition on a désigné par $\prec$, $\triangleleft$ les relations d'ordre strict associées à $\preccurlyeq$, $\trianglelefteq$ respectivement.

Proposition 5.32 *Soient* $(A, \preccurlyeq)$, $(B, \trianglelefteq)$ *ensembles ordonnés, avec* $(A, \preccurlyeq)$ *totalement ordonné. Si*

$$f : A \to B$$

est strictement monotone, alors f *est injective.*

Démonstration: On va utiliser la définition de l'injectivité. Soient a, $a' \in A$ tels que $a \neq a'$. Puisque $\preccurlyeq$ est une relation d'ordre total, on a $a \prec a'$ ou $a' \prec a$. Si f est strictement croissante le premier cas nous donne $f(a) \triangleleft f(a')$ et le deuxième cas nous donne $f(a') \triangleleft f(a)$, donc on a toujours $f(a) \neq f(a')$. Argument similaire si f est strictement décroissante. ■

Exercice 5.33 Soit $f : \mathbb{N}^* \to \mathbb{N}$ l'application définie par

$$f(n) := \text{ la somme des exposants intervenant dans la factorisation de } n \text{ en nombres premiers.}$$

Munissons $\mathbb{N}^*$ de l'ordre $|$ (divisibilité) et $\mathbb{N}$ de l'ordre usuel $\leq$. Montrer que f est strictement croissante. Est-ce qu'elle est injective ?

Exemples 5.34
1. L'application affine
$$f : \mathbb{R} \to \mathbb{R},\ f(x) = ax + b$$
est strictement croissante si $a > 0$ et strictement décroissante si $a < 0$. Donc f est injective pour tout $a \in \mathbb{R}^*$.
2. L'application $\exp : \mathbb{R} \to]0, \infty[$ est strictement croissante, donc injective.

Remarque 5.35 Soient $(A, \preccurlyeq)$, $(B, \trianglelefteq)$ ensembles ordonnés, avec $(A, \preccurlyeq)$ totalement ordonné et soit
$$f : A \to B$$
une application bijective. Si f est strictement croissante (strictement décroissante) alors la réciproque f^{-1} a la même propriété.

Démonstration: Exercice. ■

5.7 Suites et relations d'ordre

La notion de suite d'un ensemble a été introduite dans le chapitre 4.1 (voir la définition 4.8).

Définition 5.36 *Soit $(A, \preccurlyeq)$ un ensemble ordonné. Une suite $(a_n)_{n\in\mathbb{N}}$ de A est dite :*
1. *croissante, si*
$$\forall n \in \mathbb{N}\ a_n \preccurlyeq a_{n+1}.$$
2. *strictement croissante, si*
$$\forall n \in \mathbb{N}\ a_n \prec a_{n+1}.$$
3. *décroissante, si*
$$\forall n \in \mathbb{N}\ a_{n+1} \preccurlyeq a_n.$$
4. *strictement décroissante, si*
$$\forall n \in \mathbb{N}\ a_{n+1} \prec a_n.$$
5. *(strictement) monotone si elle est (strictement) croissante ou (strictement) décroissante.*
6. *majorée, s'il existe $\mu \in A$ tel que*
$$\forall n \in \mathbb{N}\ a_n \preccurlyeq \mu.$$
7. *minorée, s'il existe $\nu \in A$ tel que*
$$\forall n \in \mathbb{N}\ \nu \preccurlyeq a_n.$$
8. *bornée, si elle est majorée et minorée.*

Remarque 5.37 Une suite $(a_n)_{n\in\mathbb{N}}$ de A est croissante (strictement croissante, décroissante, strictement décroissante, monotone, strictement monotone, majorée, minorée, bornée) si et seulement si elle a cette propriété en tant que application définie sur $\mathbb{N}$ à valeurs dans A.

Exemples 5.38
1. La suite réelle $(u_n)_{n\in\mathbb{N}^*}$, $u_n = \frac{1}{n}$ est strictement décroissante et bornée.
2. La suite réelle $(u_n)_{n\in\mathbb{N}^*}$, $u_n = (-1)^n$ est bornée, mais n'est pas monotone.
3. La suite réelle $(u_n)_{n\in\mathbb{N}^*}$, $u_n = (-1)^n n$ n'est ni majorée, ni minorée, ni monotone.

6 Relations d'équivalence

Soit A un ensemble. Rappelons qu'une relation R sur A est dite relation d'équivalence si elle est réflexive, transitive et symétrique (voir la définition 3.15).

6.1 Classes d'équivalence par rapport à une relation d'équivalence. Ensemble quotient

On va commencer par la

Définition 6.1 *Deux ensembles C, D sont dits disjoints si $C \cap D = \emptyset$.*

Soit A un ensemble et soit $\mathcal{P}(A)$ l'ensemble des parties de A. Pour un *sous-ensemble* $\mathcal{Q} \subset \mathcal{P}(A)$ (donc pour un ensemble de parties de A) nous définissions

$$\bigcup_{C\in\mathcal{Q}} C := \{x \in A |\ \exists C \in \mathcal{Q},\ x \in C\},\quad \bigcap_{C\in\mathcal{Q}} C := \{x \in A |\ \forall C \in \mathcal{Q},\ x \in C\}. \tag{5}$$

Nous avons étudié des notions similaires dans le chapitre 2.3 où nous avons introduit la réunion et l'intersection *d'une famille* d'ensembles. Dans les formules (5) il ne s'agit pas d'une *famille d'ensembles*, mais d'un *ensemble de parties* d'un ensemble fixé A.

Définition 6.2 *Soit A un ensemble. Une partition (non-indexée) de A est un sous-ensemble $\mathcal{Q} \subset \mathcal{P}(A)$ tel que les conditions suivantes soient vérifiées :*

1. $$\forall C \in \mathcal{Q},\ C \neq \emptyset.$$
2. $$\bigcup_{C\in\mathcal{Q}} C = A.$$
3. $$\forall C \in \mathcal{Q}\ \forall C' \in \mathcal{Q}\ \big(C \neq C' \Rightarrow C \cap C' = \emptyset\big).$$

Donc une partition de A est une décomposition de A en réunion de sous-ensembles *non-vides et disjoints deux à deux.*

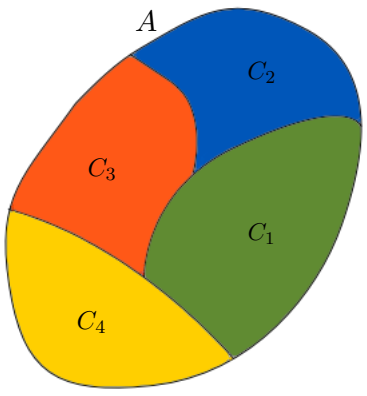


FIGURE 3 – Une partition $\{C_1, C_2, C_3, C_4\}$ d'un ensemble $A \subset \mathbb{R}^2$. Un puzzle à 4 pièces.

Exemples 6.3

1. Le sous-ensemble $\mathcal{Q} = \{]-\infty, 0],]0, \infty[\} \subset \mathcal{P}(\mathbb{R})$ est une partition de $\mathbb{R}$.
2. Soit A un ensemble et soit $\mathcal{S} := \{\{a\} |\ a \in A\} \subset \mathcal{P}(A)$ l'ensemble des singletons de A. $\mathcal{S}$ est une partition de A. Remarquer que $\mathcal{S}$ est vide si A est vide.
3. Soit $B \subset A$ un sous-ensemble de A tel que $B \neq \emptyset$ et $B \neq A$. Alors $\{B, {}^cB\}$ est une partition de A.

4. Soient
$$2\mathbb{Z} := \{2k |\ k \in \mathbb{Z}\},\ 2\mathbb{Z}+1 := \{2k+1 |\ k \in \mathbb{Z}\}$$
les ensembles des nombres entiers pairs, respectivement impairs. Alors $\{2\mathbb{Z}, 2\mathbb{Z}+1\}$ est une partition de $\mathbb{Z}$.

Définition 6.4 *Soit R une relation d'équivalence sur A.*

1. *Soit $a \in A$. La classe d'équivalence de a par rapport à R est le sous-ensemble de A défini par*
$$[a]_R := \{b \in A |\ a\ R\ b\}.$$
Donc la classe d'équivalence $[a]_R$ est l'ensemble de tous les éléments de A qui sont R-équivalents à a.
2. *Un sous-ensemble $C \subset A$ est dit classe d'équivalence par rapport à R s'il existe $a \in A$ tel que $C = [a]_R$.*
3. *L'ensemble quotient de A par R est l'ensemble A/R des classes d'équivalence par rapport à R :*
$$A/R := \{C \in \mathcal{P}(A) |\ \exists a \in A,\ C = [a]_R\}.$$
4. *La surjection canonique $p_R : A \to A/R$ est définie par*
$$p_R(a) := [a]_R,$$
donc p_R associe à un élément $a \in A$ sa classe d'équivalence $[a]_R$.

Exercice 6.5 Expliquer pourquoi p_R est bien surjective.

La proposition suivante montre que, dans la présence d'une relation d'équivalence, l'ensemble quotient A/R, regardé comme sous-ensemble de $\mathcal{P}(E)$, est une partition de A.

Proposition 6.6 *Soit A un ensemble et soit R une relation d'équivalence sur A. Alors*

1. *Pour tout $a \in A$ on a*
$$a \in [a]_R\,,$$
en particulier toute classe d'équivalence par rapport à R est non-vide.
2. *Soient a, $a' \in A$ et soient $C = [a]_R$, $C' = [a']_R \in A/R$ leurs classes d'équivalence. Les propriétés suivantes sont équivalentes :*
   (a) $C \cap C' \neq \emptyset$.
   (b) $a\ R\ a'$.
   (c) $C = C'$.
   En particulier deux classes d'équivalence $C = [a]_R$, $C' = [a']_R$ sont soit égales (quand $a\ R\ a'$), soit disjointes (quand $a \not R\ a'$).
3. *On a*
$$\bigcup_{C \in A/R} C = A.$$
4. *A/R est une partition de A.*

Démonstration: 1. Soit $a \in A$. Puisque R est réflexive on a $a\ R\ a$, donc $a \in [a]_R$ par la définition de $[a]_R$.

2. On va démontrer $(a) \Rightarrow (b) \Rightarrow (c) \Rightarrow (a)$.

$(a) \Rightarrow (b)$: Soit donc $b \in C \cap C'$. Donc $b \in [a]_R$ et $b \in [a']_R$, i.e. $a\ R\ b$ et $a'\ R\ b$. En utilisant la symétrie et la transitivité de R on obtient $a\ R\ a'$.

$(b) \Rightarrow (c)$: En supposant $a\ R\ a'$ on va démontrer par double inclusion que $C = C'$. Soit $b \in C = [a]_R$. On a donc $a\ R\ b$. Puisque $a\ R\ a'$ on obtient (en utilisant la symétrie et la transitivité de R) $a'\ R\ b$ donc $b \in [a']_R = C'$. Argument similaire pour l'inclusion inverse.

$(c) \Rightarrow (a)$: Supposons $C = C'$. On a $C \cap C' = C$, qui est non-vide d'après 1.

3. L'inclusion $\cup_{C\in A/R} C \subset A$ est évidente parce toutes les classes d'équivalence C sont des sous-ensembles de A. Pour l'inclusion inverse, soit $a \in A$. D'après la première affirmation nous savons que $a \in [a]_R$, donc a appartient à sa propre classe d'équivalence (qui "participe" à la réunion $\cup_{C\in A/R} C$), donc $a \in \cup_{C\in A/R} C$.

4. En tenant compte de la définition 6.2, l'affirmation 4. est une conséquence directe de 1., 2. et 3. ■

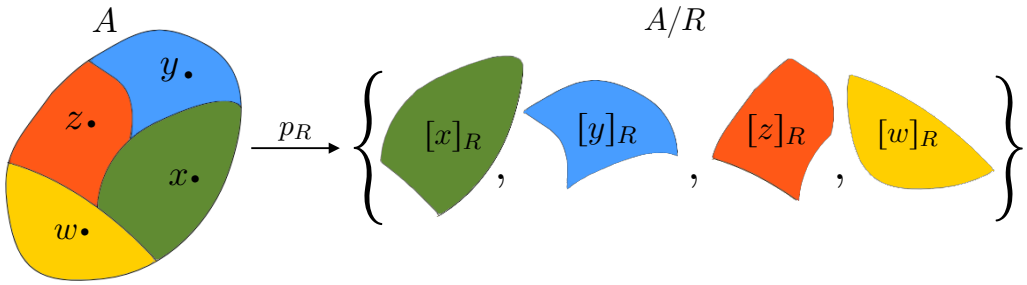


FIGURE 4 – Une relation d'équivalence R avec 4 classes d'équivalence. Chaque classe d'équivalence $C = [a]_R$ devient un élément de A/R. L'ensemble quotient A/R a 4 éléments.

En réalité la donnée d'une relation d'équivalence sur A est équivalente à la donnée d'une partition de A. La partition associée à une relation d'équivalence R est le quotient A/R regardé comme sous-ensemble de $\mathcal{P}(A)$. Le passage dans le sens contraire (d'une partition à une relation d'équivalence) est expliqué dans l'exercice suivant :

Exercice 6.7 Soit A un ensemble et soit $\mathcal{Q} \subset \mathcal{P}(A)$ une partition de A. Montrer que la relation R sur A définie par

$$a \; R \; b \text{ s'il existe } C \in \mathcal{Q} \text{ tel que } a \in C \text{ et } b \in C$$

est une relation d'équivalence sur A dont l'ensemble quotient A/R est $\mathcal{Q}$.

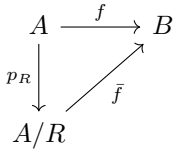
Définition 6.8 *Soit R une relation d'équivalence sur A. Une application $f : A \to B$ est dite compatible avec R si*

$$\forall x \in A \; \forall y \in A \; \big(x \; R \; y \Rightarrow f(x) = f(y)\big).$$

Exemples 6.9

1. Soit R la relation d'équivalence sur $\mathbb{Z}$ définie par : $x \; R \; y$ si $y - x \in 2\mathbb{Z}$ (i.e. si x et y sont de même parité). L'application $f : \mathbb{Z} \to \{\pm 1\}$ définie par $f(k) = (-1)^k$ est compatible avec R.
2. Soit R la relation d'équivalence sur $\mathbb{R}$ définie par : $s \; R \; t$ si $t - s \in \mathbb{Z}$. L'application $f : \mathbb{R} \to \mathbb{C}$ définie par $f(t) := e^{2\pi i t}$ est compatible avec R.

Remarque 6.10 Soient R une relation d'équivalence sur A et $f : A \to B$ une application compatible avec R. La formule $[x]_R \mapsto f(x)$ définit une application $\bar{f} : A/R \to B$ sur l'ensemble quotient A/R.



Cette application a la propriété $\bar{f} \circ p_R = f$.

Démonstration: Exercice. ■

On peut reformuler cette remarque de la manière suivante : si f est compatible avec R, alors f "descend" au quotient A/R. On va dire aussi que $\bar{f}$ est l'application *induite* par f sur le quotient A/R.

6.2 Exemples élémentaires de relations d'équivalence

Voici quelques exemples élémentaires de relations d'équivalence. Dans chaque cas on va préciser les classes d'équivalence et l'ensemble quotient.

La relation "même année de naissance" sur l'ensemble des étudiants de ce groupe. Soit $\mathcal{G}$ ce groupe d'étudiants (ici présents). Considérons la relation R sur $\mathcal{G}$ définie par

$$x \; R \; y \text{ si } x, \; y \text{ sont nés la même année.}$$

C'est facile de voir que R est une relation d'équivalence sur $\mathcal{G}$. La classe d'équivalence $[x]_R$ de $x \in \mathcal{G}$ est l'ensemble formé par lui-même et tous ses collègues nés la même année. Combien de classes d'équivalence par rapport à R y a-t-il dans votre groupe ?

La relation d'égalité Δ sur A. Soit A un ensemble. Rappelons que la relation d'égalité sur A correspond à la diagonale $\Delta := \Delta_A \subset A \times A$ du produit cartésien $A \times A$. Par rapport à cette relation, un élément $a \in A$ est en relation avec lui-même et seulement avec lui même. Pour tout élément $a \in A$ la classe d'équivalence $[a]_\Delta$ par rapport à cette relation coïncide avec le singleton $\{a\}$. Dans ce cas

$$A/\Delta = \{\{a\}|\ a \in A\}$$

est l'ensemble des singletons associés aux éléments de A et la surjection canonique $p_\Delta : A \to A/R$ est la bijection définie par

$$p_\Delta(a) = \{a\}.$$

La relation totale $A \times A$ sur A. Soit A un ensemble. Le produit cartésien $\Pi := A \times A$ est une relation d'équivalence sur A. Pour tout élément $a \in A$ la classe d'équivalence $[a]_\Pi$ par rapport à cette relation coïncide avec A. L'ensemble quotient A/Π est le singleton $\{A\}$ et la surjection canonique est l'application constante $p_\Pi : A \to \{A\}$ donnée par $p_\Pi(a) = A$ pour tout $a \in A$.

La relation "de même parité" sur $\mathbb{Z}$. Soient $a, b \in \mathbb{Z}$. La condition "a, b sont de même parité" définit une relation d'équivalence R_{par} sur $\mathbb{Z}$. Remarquons que $a \; R_{\text{par}} \; b$ si et seulement si $b - a$ est pair, donc R_{par} coïncide avec la relation de congruence mod 2 (voir l'exemple 3.4 et la remarque 3.6).

La classe d'équivalence d'un nombre pair est $2\mathbb{Z} := \{2k|\ k \in \mathbb{Z}\}$ et la classe d'équivalence d'un nombre impair est $2\mathbb{Z} + 1 := \{2k + 1|\ k \in \mathbb{Z}\}$. Le quotient $\mathbb{Z}/R_{\text{par}}$ est donc

$$\mathbb{Z}/R_{\text{par}} = \{2\mathbb{Z}, 2\mathbb{Z} + 1\},$$

et la surjection canonique $p_{R_{\text{par}}} : \mathbb{Z} \to \mathbb{Z}/R_{\text{par}}$ est donnée par

$$p_{R_{\text{par}}}(x) = \begin{cases} 2\mathbb{Z} & \text{si} \quad x \text{ est pair} \\ 2\mathbb{Z} + 1 & \text{si} \quad x \text{ est impair} \end{cases}.$$

Le relation "de même signe" sur $\mathbb{R}^*$. Soient $x, y \in \mathbb{R}^*$. La condition "x, y sont de même signe" définit une relation d'équivalence R_{sign} sur $\mathbb{R}^*$. Remarquons que $x \; R_{\text{sign}} \; y$ si et seulement si $xy > 0$. La classe d'équivalence d'un nombre strictement positif est $\mathbb{R}^*_+$ et la classe d'équivalence d'un nombre strictement négatif est $\mathbb{R}^*_-$. Le quotient $\mathbb{R}^*/R_{\text{sign}}$ est donc

$$\mathbb{R}^*/R_{\text{sign}} = \{\mathbb{R}^*_-, \mathbb{R}^*_+\},$$

et la surjection canonique $p_{R_{\text{sign}}} : \mathbb{R}^* \to \mathbb{R}^*/R_{\text{sign}}$ est donnée par

$$p_{R_{\text{sign}}}(x) = \begin{cases} \mathbb{R}^*_+ & \text{si} \quad x > 0 \\ \mathbb{R}^*_- & \text{si} \quad x < 0. \end{cases}.$$

Le relation "même image par f" sur l'ensemble de définition de f. Soit $f : A \to B$ une application. La relation d'équivalence associée à f est la relation R_f sur A définie par

$$x \; R_f \; x' \text{ si } f(x) = f(x').$$

La classe d'équivalence d'un élément $a \in A$ est

$$[a]_{R_f} = \{x \in A |\; f(x) = f(a)\} = \{x \in A |\; f(x) \in \{f(a)\}\} = f^{-1}(\{f(a)\}).$$

Donc la classe d'équivalence de a par rapport à R_f est l'image réciproque $f^{-1}(\{f(a)\})$ du singleton $\{f(a)\}$. Cette image réciproque s'appelle *la fibre de f au-dessus de $f(a)$*, ou la fibre de f qui passe par a.

Remarque 6.11 La formule

$$\bar{f}([x]_{R_f}) = f(x) \tag{6}$$

définit une bijection

$$\bar{f} : A/R_f \to \mathrm{Im}(f).$$

Démonstration: Il faut d'abord vérifier que $\bar{f}$ est bien définie, i.e. que le membre droit de (6) dépend seulement de la classe d'équivalence $[x]_{R_f}$. Il faut donc vérifier que si on choisit un autre "représentant" x' de la même classe, on aura $f(x) = f(x')$. Mais $x' \in [x]_{R_f}$ si et seulement si $x \; R_f \; x'$, si et seulement si $f(x) = f(x')$. Vérifier l'injectivité et la surjectivité de $\bar{f}$. ■

La signification de la remarque 6.11 est : l'ensemble quotient A/R_f "s'identifie" naturellement à l'image $\mathrm{Im}(f)$ de f.

Exercice 6.12 Soit $f : \mathbb{R} \to \mathbb{R}$ définie par $f(x) = \cos(x)$. Pour un élément $x \in \mathbb{R}$ écrire explicitement la classe d'équivalence $[x]_{R_f}$. La même question pour l'application $g : \mathbb{R} \to \mathbb{R}$, $g(x) = \sin(x)$.

Exercice 6.13 Soient A un ensemble et R une relation d'équivalence sur A. Quelle est la relation d'équivalence R_{p_R} associée à la surjection canonique $p_R : A \to A/R$? En déduire que *toute* relation d'équivalence sur A est associée à une application définie sur A.

Exercice 6.14 Soit $f : A \to B$ une application. Montrer que f s'écrit comme la composée $\iota \circ \bar{f} \circ p_{R_f}$, où $p_{R_f} : A \to A/R_f$ est la surjection canonique associée à la relation d'équivalence R_f, $\bar{f} : A/R_f \to \mathrm{Im}(f)$ est la bijection mise en évidence dans la remarque 6.11 et $\iota : \mathrm{Im}(f) \hookrightarrow B$ est l'application d'inclusion, qui est évidemment injective. On obtient donc le diagramme

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & B \\ {\scriptstyle \text{surj.}}\downarrow{\scriptstyle p_{R_f}} & & \uparrow{\scriptstyle \iota}\,{\scriptstyle \text{inj.}} \\ A/R_f & \xrightarrow[\text{bij.}]{\bar{f}} & \mathrm{Im}(f)\ . \end{array} \tag{7}$$

L'égalité $f = \iota \circ \bar{f} \circ p_{R_f}$ nous dit que *ce diagramme est commutatif*, i.e. les deux applications $A \to B$ obtenues en composant les applications indiquées par les flèches, coïncident.

6.3 Le quotient $\mathbb{Z}/n\mathbb{Z}$

Soit $n \in \mathbb{N}^*$ et soit

$$n\mathbb{Z} := \{nk |\; k \in \mathbb{Z}\}$$

l'ensemble des multiples entiers de n. Plus généralement, pour $x \in \mathbb{Z}$ posons

$$x + n\mathbb{Z} = \{x + nk |\; k \in \mathbb{Z}\}.$$

Rappelons que la relation de congruence mod n sur $\mathbb{Z}$ est définie par

$$x \equiv y \,[n] \text{ si } n|(y - x), \tag{8}$$

et que cette relation est une relation d'équivalence sur $\mathbb{Z}$. En effet, d'après la remarque 3.6 il en résulte que $x \equiv y\,[n]$ si et seulement si le reste de la division euclidienne de x par n coïncide avec le reste de la division euclidienne de y par n. Il en résulte que la relation de congruence mod n sur $\mathbb{Z}$ coïncide avec la relation R_{r_n} associée à l'application $r_n : \mathbb{Z} \to \{0, \ldots, n-1\}$ définie par

$$r_n(x) = \text{ le reste de la division euclidienne de } x \text{ par } n\,.$$

En tant que relation associée à une application, cette relation sera bien une relation d'équivalence.

Afin de pouvoir utiliser de manière homogène les notations introduites dans le chapitre 6.1, désignons par $\underset{n}{\equiv}$ cette relation d'équivalence. La définition (8) devient :

$$x \underset{n}{\equiv} y \text{ si } y - x \in n\mathbb{Z}\,. \tag{9}$$

La classe d'équivalence d'un élément $x \in \mathbb{Z}$ par rapport à $\underset{n}{\equiv}$ sera donc

$$[x]_n = \{y \in \mathbb{Z} |\ x \underset{n}{\equiv} y\} = \{y \in \mathbb{Z} |\ \exists k \in \mathbb{Z},\ y = x + nk\} = x + n\mathbb{Z},$$

en particulier la classe de 0 (la classe triviale mod n) est

$$[0]_n = n\mathbb{Z}.$$

Notre but est de comprendre en détail l'ensemble quotient $\mathbb{Z}/\underset{n}{\equiv}$. La notation standard pour cet ensemble quotient est $\mathbb{Z}/n\mathbb{Z}$ et cette notation est justifiée par la formule (9).

Proposition 6.15 *Soit $n \in \mathbb{N}^*$.*

1. *L'application $\gamma : \{0, \ldots, n-1\} \to \mathbb{Z}/n\mathbb{Z}$ définie par $\gamma(k) = [k]_n$ est bijective.*
2. *Les classes d'équivalence $[0]_n, \ldots, [n-1]_n$ sont distinctes deux à deux et l'ensemble quotient $\mathbb{Z}/n\mathbb{Z}$ s'écrit explicitement*
$$\mathbb{Z}/n\mathbb{Z} = \{[0]_n, \ldots, [n-1]_n\}.$$
En particulier $\operatorname{card}(\mathbb{Z}/n\mathbb{Z}) = n$.

Démonstration: On va utiliser la remarque 4.30, plus précisément on va construire une application

$$\rho : \mathbb{Z}/n\mathbb{Z} \to \{0, \ldots, n-1\}$$

telle que

$$\gamma \circ \rho = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}},\ \rho \circ \gamma = \mathrm{id}_{\{0,\ldots,n-1\}}.$$

L'application ρ est définie de la manière suivante : pour une classe $\xi = [k]_n \in \mathbb{Z}/n\mathbb{Z}$ posons

$$\rho(\xi) = \text{ le reste de la division euclidienne de } k \text{ par } n \tag{10}$$

(voir le théorème 3.5). Remarquons d'abord que ρ est bien définie. En effet, si on remplace k par un autre "représentant" k' de la classe ξ, on aura $k' - k \in n\mathbb{Z}$, donc le reste de la division euclidienne de k' par n coïncide avec le reste de la division euclidienne de k par n. Ceci montre que le membre droit de (10) dépend seulement de ξ.

L'égalité $\rho \circ \gamma = \mathrm{id}_{\{0,\ldots,n-1\}}$ est évidente. Démontrons l'égalité $\gamma \circ \rho = \mathrm{id}_{\mathbb{Z}/n\mathbb{Z}}$, i.e. $\gamma(\rho([k]_n)) = [k]_n$ pour tout $k \in \mathbb{Z}$. Il suffit de remarquer que k et le reste de la division euclidienne de k par n sont congrus mod n, donc leurs classes mod n coïncident.

2. Est une conséquence directe de 1. Préciser les détails. ∎

Exemple 6.16 Pour $n = 5$ on obtient $\mathbb{Z}/5\mathbb{Z} = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$. Montrer qu'on a aussi

$$\mathbb{Z}/5\mathbb{Z} = \{[33]_5, [56]_5, [27]_5, [15]_5, [29]_5\}.$$

6.3.1 Les opérations $+$, $\cdot$ sur $\mathbb{Z}/n\mathbb{Z}$.

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ est intéressant du point de vue de l'algèbre moderne parce qu'il peut être muni naturellement de deux opérations : l'addition et la multiplication des classes de congruence. Ces opérations sont "induites" par les opérations élémentaires sur $\mathbb{Z}$, mais ne sont pas des opérations avec des nombres. Ce sont des opérations algébriques nouvelles.

L'addition sur $\mathbb{Z}/n\mathbb{Z}$ est définie par

$$[x]_n + [y]_n := [x+y]_n.$$

Cette définition est cohérente, au sens que le membre droit $[x+y]_n$ dépend seulement des classes $[x]_n$, $[y]_n$, pas des représentants x, y de ces classes. En effet, si on choisit d'autres représentants x', y' de ces classes (c'est à dire $[x']_n = [x]_n$, $[y']_n = [y]_n$), alors il existe $k \in \mathbb{Z}$, $l \in \mathbb{Z}$ tels que $x' - x = kn$, $y' - y = ln$, donc $(x'+y') - (x+y) = (k+l)n \in n\mathbb{Z}$, donc $[x'+y']_n = [x+y]_n$.

De manière similaire, la multiplication sur $\mathbb{Z}/n\mathbb{Z}$ est définie par

$$[x]_n \cdot [y]_n := [xy]_n.$$

Exercice 6.17 Montrer que la définition de la multiplication est cohérente. Plus précisément, montrer que si $[x']_n = [x]_n$ et $[y']_n = [y]_n$, alors $[x'y']_n = [xy]_n$.

Exercice 6.18 Compléter les tables des deux opérations sur $\mathbb{Z}/7\mathbb{Z}$:

$+$	$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[0]_7$	$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[1]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$	$[0]_7$
$[2]_7$	$[2]_7$						
$[3]_7$	$[3]_7$						
$[4]_7$	$[4]_7$						
$[5]_7$	$[5]_7$						
$[6]_7$	$[6]_7$						

$\cdot$	$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[0]_7$	$[0]_7$	$[0]_7$	$[0]_7$	$[0]_7$	$[0]_7$	$[0]_7$	$[0]_7$
$[1]_7$	$[0]_7$	$[1]_7$	$[2]_7$	$[3]_7$	$[4]_7$	$[5]_7$	$[6]_7$
$[2]_7$	$[0]_7$						
$[3]_7$	$[0]_7$						
$[4]_7$	$[0]_7$						
$[5]_7$	$[0]_7$						
$[6]_7$	$[0]_7$						

.

En utilisant les propriétés élémentaires de l'addition et de la multiplication sur $\mathbb{Z}$ on obtient facilement :

Proposition 6.19 *Les opérations $+$ et $\cdot$ sur $\mathbb{Z}/n\mathbb{Z}$ satisfont les propriétés suivantes :*

1. *L'addition est associative :*

$$\forall(\alpha,\beta,\gamma) \in (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),\ (\alpha+\beta)+\gamma = \alpha+(\beta+\gamma).$$

2. *La classe nulle $[0]_n$ est élément neutre pour l'addition :*

$$\forall\alpha \in \mathbb{Z}/n\mathbb{Z},\ \alpha + [0]_n = [0]_n + \alpha = \alpha.$$

3. *Pour toute classe $\alpha = [k]_n \in \mathbb{Z}/n\mathbb{Z}$ la classe $-\alpha := [-k]_n$ est un élément symétrique de α par rapport à l'addition :*

$$\alpha + (-\alpha) = [0]_n.$$

4. *L'addition est commutative :*

$$\forall(\alpha,\beta) \in (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),\ \alpha+\beta = \beta+\alpha.$$

5. *La multiplication est associative :*

$$\forall(\alpha,\beta,\gamma) \in (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),\ (\alpha\cdot\beta)\cdot\gamma = \alpha\cdot(\beta\cdot\gamma).$$

6. *La classe* $[1]_n$ *est élément neutre pour la multiplication :*

$$\forall \alpha \in \mathbb{Z}/n\mathbb{Z},\ \alpha \cdot [1]_n = [1]_n \cdot \alpha = \alpha.$$

7. *La multiplication est commutative :*

$$\forall (\alpha, \beta) \in (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),\ \alpha \cdot \beta = \beta \cdot \alpha.$$

8. *La multiplication est distributive par rapport à l'addition :*

$$\forall (\alpha, \beta, \gamma) \in (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z}),\ \alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma.$$

Remarque 6.20 La multiplication des nombres (dans $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$) a une propriété très importante : le produit de deux éléments non-nuls est toujours non-nul. Une difficulté importante : si $n \geq 2$ n'est pas un nombre premier, cette propriété *n'est pas vraie dans* $\mathbb{Z}/n\mathbb{Z}$.

Exemple 6.21 Dans $\mathbb{Z}/6\mathbb{Z}$ nous avons : $[2]_6 \neq [0]_6$, $[3]_6 \neq [0]_6$, mais $[2]_6 \cdot [3]_6 = [0]_6$.

Exercice 6.22 1. Donner la liste de tous les couples $(\lambda, \eta) \in (\mathbb{Z}/12\mathbb{Z}) \times (\mathbb{Z}/12\mathbb{Z})$ tels que $\lambda \cdot \eta = [0]_{12}$.

2. Résoudre l'équation

$$x^2 - ([5]_{12})x + [6]_{12} = [0]_{12}$$

dans $\mathbb{Z}/12\mathbb{Z}$.

Exercice 6.23 Soit $n \in \mathbb{N}^*$, $n \geq 2$ et soit $a \in \mathbb{Z}^*$. Les conditions suivantes sont équivalentes :

1. La classe $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ est inversible par rapport à la multiplication, i.e. il existe une classe $[b]_n \in \mathbb{Z}/n\mathbb{Z}$ telle que $[a]_n \cdot [b]_n = [1]_n$.
2. $\text{pgcd}(a, n) = 1$.

Indication : Utiliser le théorème de Bézout (le corollaire 6.25).

6.3.2 Rappel : l'égalité et le théorème de Bézout

La définition (5.22) du pgcd et du ppcm de deux naturels non-nuls se généralise pour un couple *d'entiers* non-nuls. Pour un couple $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$ nous avons

$$\text{pgcd}(m, n) = \text{pgcd}(|m|, |n|) \in \mathbb{N}^*,\ \text{ppcm}(m, n) = \text{ppcm}(|m|, |n|) \in \mathbb{N}^*.$$

Théorème 6.24 (L'égalité de Bézout) *Soit* $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. *Alors il existe un couple* $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ *tel que*

$$\text{pgcd}(m, n) = um + vn.$$

En utilisant la notation $m\mathbb{Z} + n\mathbb{Z} := \{um + vn |\ (u, v) \in \mathbb{Z} \times \mathbb{Z}\}$, le théorème 6.24 s'écrit :

$$\text{pgcd}(m, n) \in m\mathbb{Z} + n\mathbb{Z}\,.$$

Démonstration: Posons

$$\mathcal{E} := \{k \in \mathbb{N}^* |\ \exists (u, v) \in \mathbb{Z} \times \mathbb{Z} \text{ telle que } k = um + vn\} = (m\mathbb{Z} + n\mathbb{Z}) \cap \mathbb{N}^*\,.$$

Remarquer que $\mathcal{E}$ est un sous-ensemble non-vide de $\mathbb{N}^*$ (pourquoi ?). D'après le théorème 5.7 il en résulte que le minimum $\delta := \min(\mathcal{E})$ existe. Puisque $\delta \in \mathcal{E}$ on a

$$\delta = u_\delta m + v_\delta n$$

avec $(u_\delta, v_\delta) \in \mathbb{Z} \times \mathbb{Z}$. Nous allons montrer que $\delta = \text{pgcd}(m, n)$. Il suffit de démontrer que

(a) δ est un diviseur commun de m et n.

(b) Tout diviseur commun de m et n est un diviseur de δ.

Pour démontrer (a) appliquons le théorème de division euclidienne (théorème 3.5) aux couples (δ, m) et (δ, n). On obtient

$$m = q\delta + r,\ n = q'\delta + r'\,,$$

où $(q, q') \in \mathbb{Z} \times \mathbb{Z}$, $0 \leq r < \delta$, $0 \leq r' < \delta$. Nous allons montrer (par l'absurde) que $r = r' = 0$. En effet, supposons par exemple $r > 0$. Alors

$$\mathbb{N}^* \ni r = m - q\delta = m - q(u_\delta m + v_\delta n) = (1 - qu_\delta)m + (-qv_\delta)n\,,$$

qui, évidemment, est un élément de $\mathcal{E}$. Mais on a $r < \delta$, ce qui contredit la définition de δ (le minimum de l'ensemble $\mathcal{E}$). Il en résulte $r = 0$. Un argument similaire donne $r' = 0$. Donc $r = r' = 0$, ce qui implique évidemment $\delta | m$ et $\delta | n$.

Pour démontrer (b) soit $d \in \mathbb{Z}^*$ diviseur commun de m et n. Alors $d | u_\delta m$ et $d | v_\delta n$, donc $d | (u_\delta m + v_\delta n) = \delta$. ■

Rappelons que deux entiers non-nuls m, n sont dits premiers entre eux si $\text{pgcd}(m, n) = 1$.

Corollaire 6.25 (Le théorème de Bézout) *Soit $(m, n) \in \mathbb{Z}^* \times \mathbb{Z}^*$. Alors m, n sont premiers entre eux si et seulement s'il existe un couple $(u, v) \in \mathbb{Z} \times \mathbb{Z}$ tel que $um + vn = 1$.*

Références

[Chi] R. Chill : Logique et théorie des ensembles, Université de Metz 2007/2008, `http://www.math.univ-metz.fr/~chill/logique.pdf`.

[Mer] D.-J. Mercier : PREPA CAPES MATHS 2016, Algèbre & Arithmétique, CSIPP (2015), ISBN-13 : 978-1514852538.

[Exo7] Exo7. Cours et exercices de mathématiques, `http://exo7.emath.fr/cours/cours-exo7.pdf`.